Does traditional security risk assessment have a future in information security?

Ruighaver, A. B., Warren, M. and Ahmad, A. 2011, Does traditional security risk assessment have a future in information security? *Journal of information warfare*, vol. 10, no. 3, pp. 16-28.

Does traditional security risk assessment have a future in Information Security?

A. B. Ruighaver[1], M. Warren[1] and A. Ahmad[2],

[1] *School of Information Systems, Deakin University, Australia*
Email: {tobias, matthew.warren} @deakin.edu.au

[2] *Department of Computing and Information Systems, University of Melbourne, Australia*
Email: atif@unimelb.edu.au

Abstract.

The current information security standards still advocate the use of risk assessment in the prioritisation of security investments. However, prior research on the use of risk assessment methodologies in organisational security has shown that the use of the traditional monolithic risk assessment process described in the current risk management standard is simply not practical at the organisational level. This paper first examines the problems in performing a systematic risk assessment and then discusses the limitations of a traditional risk assessment. To address these limitations, this paper proposes splitting up the current monolithic risk assessment process. The result is an information security assessment framework that puts greater emphasis on situational awareness and allows for better decision making on the prioritization of security investments.

Keywords: information security, risk management, security assessment, security requirements.

Introduction

Traditional approaches to information security, including the current information security management standards, are still promoting the belief that information security is in principal a risk management process. While risk management undoubtedly plays a role in information security, there are many other aspects that need to be considered in the management of information security. In particular, the increase in complexity of information security and the number of controls recommended by the current standards means that the economics of information security is now of growing concern and prioritising security investment on risk alone may no longer be an effective solution.

Over the past decades the growing complexity of Information Communications Technology (ICT) infrastructures in organizations has driven up the cost of enterprise risk assessment (PITAC, 2005). In a previous paper, Shedden *et al* (2006) discussed how some organisations actually perform risk assessment and showed how the enormous complexity and cost simply made it impractical to perform a thorough systematic risk assessment.

Shedden et.al. found that the need to reduce the cost of conducting a full scale systematic assessment typically results in organisations developing their own internal risk assessment processes. Although these processes were derived from the best-practice standards such as the AS/NZS 4360 (1999), they were radically simplified. Some of the problems identified in our case studies, such as inadequate knowledge and guidance, incorrect granularity of asset identification and misalignment of outcomes (Shedden *et al.*, 2006), put serious doubt on

SSN 1445-3312 print/ISSN 1445-3347 online

whether the outcomes of these risk assessments should be used in decision making and, in particular, for the selection of security controls.

In practice, as shown by these case studies, the risk assessment process is often only used to assist the organisation in audits, legislation compliance and transference of responsibility. Organisations frequently select their security controls directly from the controls listed in the security standard ISO 17799 or its successor ISO27002. Lack of concrete prioritisation guidelines or security strategies does not only mean that the final selection is often based on personal preference of the decision maker but, as a result of this practice, there has also been a serious lack of innovation in information security. The controls listed in security standards have not significantly changed over the past two decades, while over the same period the security and risk environment has changed dramatically.

Our experience in these case studies on risk assessment in Australian organizations led to further research into organizational learning and incident handling. An initial case study followed by a focus group (to be published in a later paper) has confirmed a general lack of feedback from incident handling into risk assessment. Organizational learning in incident handling does in general only aim to improve incident handling itself, but will sometimes suggest new security controls in an attempt to reduce the number of incidents. Not only did we find no evidence of any feedback from incident handling to improve the artefacts used in the organization's risk assessment process, the focus group showed a surprising reluctance to even consider that root cause analysis in incident handling could (or should) also analyse the actual risk assessment process used to prioritize and select security controls.

This paper begins by addressing the use of traditional risk assessment to prioritise the implementation of information security controls. The next section identifies several additional limitations of traditional risk assessment. To illustrate an alternative to the current monolithic risk assessment process this paper will further examine the artefacts produced by traditional risk assessment, extend these artefacts and identify alternative methods to produce and maintain these artefacts. The final section will then identify several research areas that need urgent attention.

The Problem with Traditional Security Risk Assessment

Traditional security risk assessment is seen as a single monolithic process that aims to provide a systematic approach to identify, assess and treat risks (HB 231, 2004). Hence, the outcome of a security risk assessment is expected to include a list of the most critical information assets, a comprehensive evaluation of the threats and vulnerabilities that would endanger each of these assets, an estimate of the likelihood and consequences of these threats exposing these vulnerabilities, and finally the controls that are needed to mitigate, avoid or transfer these risks in the most cost effective way (Visintine, 2003) (Whitman and Mattord, 2005).

A generic security risk assessment process generally consists of:

- Describing the scope and context of the risk assessment
- Identifying Critical assets
- For each asset identifying the relevant vulnerabilities
- For each vulnerability identifying the relevant threats
- For each pair of vulnerability and threat identifying the likelihood and impact
- Identifying the controls needed

The Cost of a Systematic Risk Assessment

The quality of a risk assessment depends on how systematically this approach has been applied and documented. If an asset has not been identified, or classified as non-critical, it is unlikely that it will be protected. If a threat or vulnerability has not been identified, or considered irrelevant, the asset will probably not be protected against that particular risk.

A comprehensive systematic risk evaluation of even a single asset is a massive undertaking. Assuming the risk assessment process produces a complete list of all possible threats and vulnerabilities, systematically evaluating each relevant threat for every possible vulnerability, as well as estimating the likelihood and impact for each combination is a costly exercise. And, if this process needs to be repeated for each data asset, then the task becomes largely intractable as data assets are transferred over networks and printed.

In practice, a full list of potential threats and vulnerabilities is rarely available. Interviews with stakeholders are often used to identify risks from an historical perspective and only the threats and vulnerabilities in these risks are considered relevant. Although this is a cost-effective way to perform a risk assessment and an effective way to concentrate security efforts on preventing re-occurrence of past incidents, this is not a systematic approach and it indicates the failure of a pure risk management based approach to security. If the necessary feedback and organisational learning loops in incident handling had been implemented, the historical data on what assets have been compromised by what threats and vulnerabilities would have been available without the need for interviews. At the same time, the necessary controls to reduce these risks would also already been identified and implemented.

Selection of Controls

Unfortunately, even if a full systematic evaluation of all relevant threats and vulnerabilities has been performed, there may, in general, not be an easy way to use this information to assist in the selection of the best control. Moreover, most security controls will cover a large range of risks (and assets), so it may not have been necessary to evaluate the likelihood and impact of every risk after all.

In practice, it might have been better to select a control before the comprehensive risk evaluation takes place and use the risk evaluation process to assess which threats and/or vulnerabilities are not covered by this control. This trial and error approach seems to work reasonably well and now it will only be necessary to estimate the likelihood and impact for a few remaining threats and vulnerabilities to get an idea whether the residual risk is acceptable. Hence, the result is an effective, systematic, and relatively low-cost risk assessment for use in legislation compliance and transference of responsibility. Unfortunately, the use of a trial and error approach to select controls does not necessarily result in the most cost-effective solution for information security and neither does it necessarily encourage innovation.

Identification of Critical Assets

Having discussed the problem of using a risk assessment to identify the most cost-effective controls to secure a single asset, we still need to discuss the problem of how we identify the most critical assets. Unfortunately, there is no definition on what critical means in most guidelines for risk assessment and neither is there a good definition on what an asset really is. Should knowledge be treated like an asset? And what about reputation? This lack of a clear definition of what a critical asset is, does unfortunately create several problems for information security.

One would assume that a systematic approach is needed to identify critical assets. Hence, a reasonable approach would be to first identify all assets and then use a set of approved criteria (by the organisation) to rank these assets. Unfortunately, our case studies have found no evidence of such a process.

How we identify these criteria for identifying critical assets is crucial for good information security, because if we have not identified a "critical" asset, we will not be able to protect it. Unfortunately, there are no guidelines for establishing these criteria in the standards. There is even a suggestion in literature that protecting the most vulnerable assets might not be cost-effective (Gordon *and* Loeb, 2002), which will further complicate the selection of critical assets. And, finally, what do we do with the less critical assets? Since we won't be performing a risk assessment, does that mean we won't provide any controls for these assets?

Further Limitations of Traditional Risk Assessment

Even if an organisation does perform a risk assessment as discussed in section 2 at the organizational level, the impact of this assessment on the design of the organisation's security infrastructure will often be minimal. Many of the typical incidents in information security, such as network attacks, social engineering attacks or accidental information leakage, are not necessarily directly related to the critical assets identified in the risk assessment. While there are other risk assessment methodologies, such as Octave (Alberts and Dorofee, 2004), suitable for the identification of risks in IT and network infrastructure, they have similar problems (Coleman, 2004) and do not help in solving the problem of how much resources should be assigned to, for instance, network security in relation to other areas such as social engineering and information leakage.

Lack of feedback processes

Incidents, whether small or large, can be an important source of information about risk, but few organisations have enough detective controls in place to ensure they have adequate situational awareness. Although this is mainly caused by the Plan, Decide, Act (PDA) decision model (Grant *et al.*, 2005) advocated by current security standards, the emphasis on preventive controls in information security resulting from the use of PDA is not prevented by the monolithic process used in traditional risk assessment. There is no indication in the current risk assessment process on how feedback processes are to be used to check and update threat and vulnerability profiles or how incident investigation can improve asset identification and classification. The need for extensive documentation of the decisions made in a risk assessment is also not recognised, making it difficult for organisations to analyse the risk assessment process and learn of its deficiencies after an incident.

Lack of systematic identification and classification of assets

The process used in traditional risk assessment does not identify the need to analyse the information flows in the organisation. As expected, therefore, our case studies in risk assessment found no evidence that any identification of information flows took place for even the most critical data assets. This may simply be because having different assessment methods for different types of assets would make the risk assessment methodology even more complex, but in the current complex ICT infrastructures information flows have an enormous impact on the risk identification for particular assets, and not identifying information flows makes the risk identification for these assets almost worthless. Of course, as soon as we start identifying information flows (and business processes), the question arises whether we should extend the process by providing risk assessment for critical information flows and business processes as well.

Another aspect missing in traditional risk assessment is the need for the organisation to classify the identified assets for confidentiality, availability and integrity. While there is a well known classification of assets for confidentiality alone (Kailay *et al.*, 1995), no classification for availability or integrity is known to the authors. Organisations also rarely recognise the need to identify the trade off between these different aspects of security. For data assets in particular, the trade off between availability and confidentiality is extremely important and knowing the relative weight of these two aspects is essential when an organisation tries to secure its business systems and processes. Data assets that require high availability as well as high confidentiality will surely offer significantly more challenges to a security architect than data assets that only require either availability or confidentiality.

Use of a single failure approach

The final limitation of traditional risk assessment that needs to be discussed in this section is that this approach only considers risk under normal operational circumstances. It does not consider how risks to a particular asset change when an incident is in progress. It is a well known fact that major incidents are always the result of a number of successive failures. That is the reason why incident handling policies are so important, but these policies don't really become active until a major incident is already in progress. Use of what-if scenarios in risk evaluation would be one possibility, but of course that would make risk assessment even more expensive.

Risk Assessment Artefacts and their Use

In the previous sections we have identified some of the problems and limitations of the traditional monolithic risk assessment process. While this paper does not aim to offer the final solution to replace traditional risk assessment, this section will examine the artefacts that a risk assessment methodology should produce, followed by a discussion on where these artefacts could potentially be used outside the risk assessment process itself.

Apart from a short description of the process used, the only other artefact commonly found in the organisations that we have investigated is a final ranked list of risks that the organisation expects to control. Many of the other artefacts used to produce this ranked list are often poorly documented, if they still exist at all.

Assets to be Protected

In our view, the first and often most important artefact that needs to be produced to ensure a high-quality risk assessment is the list of assets to be used in the critical asset identification stage. Our case studies showed a clear failure in the organizations we studied to systematically identify and document their assets at a level of granularity low enough to enable effective identification and protection of critical assets (Shedden *et al.*, 2006)

Currently a common approach seems to be to identify the critical business processes first and then assume that the assets used in these processes are likely critical assets. The German Grundschutz methodology (Jaschob, 2006), for instance, emphasizes the identification and analysis of business processes as the main focus in the design and planning of a security process. It then proposes a security level assessment for each process to guide the creation of the organisation's policy for information security. An actual risk assessment is only suggested for those business processes that have a very high security requirement that may not be satisfied by the implementation of the standard security modules available in this Grundschutz methodology.

If an organization does not know which assets have been discarded in the selection of critical assets (and why), it will be difficult to thoroughly evaluate the quality of the process used for the selection of critical assets. While the initial identification of business processes in an organisation can assist in ensuring that a complete list of assets will be assembled, many current risk assessment methods like the Grundschutz methodology do not explicitly mention the need to produce a list of assets, nor do they encourage the classification of assets from a security aspects point of view.

A list of assets and a classification of what they need to be protected from (confidentiality, integrity and/or availability) will also be a valuable tool in the organisation's security awareness program. Instead of making staff aware how sensitive some of the assets are that they commonly use, current awareness programs often only concentrate on a few relevant risks and attempt to change the employee's attitude in relation to these risks (Wipawayangkool, 2009). Again, our research indicates that staff members are often not aware of the sensitivity of the assets they are using in their daily tasks.

Changing the focus of the organisation's awareness training to ensure that staff are aware which assets under their control need the most protection could well be one of the most effective controls an organisation can apply. Research by Norman (2001), for instance, found that to protect knowledge in a partnership alliance the most effective approach was to simply make personnel aware of the need to protect certain knowledge and to identify what knowledge needed protection.

It is important that the classification of assets also takes into account the potential impact on the reputation of the company if the security of an asset is compromised. Instead of treating reputation as an asset in a risk assessment, it will be easier to treat it as a potential impact. However, as reputation is probably the most valuable asset of an organisation, initiating a separate consequence analysis to identify the sensitivity of assets in relation to the organisation's reputation will ensure that securing these assets will get high priority in the selection of security controls.

Threats and Vulnerabilities

Over the past decade the number of threats and vulnerabilities that need to be considered in a systematic risk assessment has increased significantly. While there are many sources that will enable an organization to collect an extensive list of potential threats and vulnerabilities, bringing that list down to a reasonable sized list of the most relevant threats and vulnerabilities for that organisation is, however, not easy. Most risk assessment methodologies still rely on interviews within the organisation to determine the relevant threats and vulnerabilities (Alberts and Dorofee, 2004) (Jaschob *et al.*, 2006), but little research is available on the quality of the information produced in that process considering the current dynamic threat environment as well as the increasingly complex ICT infrastructure of organisations.

An accurate view of the most relevant threats and vulnerabilities for an organisation is often lacking as most organisations don't have the necessary monitoring and reporting procedures in place to collect data about which threats and vulnerabilities are currently impacting on the organisation's security. Situational awareness is an important tool in safety (Endsley *et al.*, 1995), but the emphasis on prevention in current Information Security standards has focused situational awareness in organisations on compliance instead of on their security failures. Authentication and access control, for instance, are some of the most basic controls in

Information Security and are known to be a weak link in most organisations (Sasse *et al.*, 2001). Still, the application of detective controls that will inform the organisation when these controls are compromised is almost non-existent (Ruighaver, 2010).

To improve situational awareness in the current dynamic security environment we need to identify and communicate which threats are currently impacting the organisation and which vulnerabilities they are currently exploiting and which they are likely to exploit in the future. Improved decision making in a dynamic environment depends on an accurate and complete view of the current situation (Endsley, 1995) and one can expect therefore that organisation will need to put more effort in the collection of an extensive list of potential threats and vulnerabilities as well as in the process of identifying which of these threats and vulnerabilities are relevant for their particular organisation.

Available Controls

The current ISO27002 standard proposes an extensive list of controls that can be used by organisations, but does not link them to the risks they are supposed to control. As discussed in section 2, one of the major shortcomings in traditional risk assessment is the lack of a systematic approach for the selection of controls when a major risk has been identified. The Grundschutz methodology (Jaschob *et al.*, 2006) partly circumvents this problem by using a baseline approach, which proscribes modules with standard security controls. As soon as more security is needed, however, the same problem resurfaces.

Although ISO27002 is a fairly recent standard, the set of controls listed in this standard is not that different from the set listed in previous standards such as ISO/IEC 17799. In the recent decade, however, the ICT infrastructures used in organisations as well as their connection to external organisations and the Internet has changed significantly. Hence, a search through recent literature, or a simple brainstorming session with anyone involved in information security, is likely to come up with a range of potential controls that is not currently listed in ISO27002.

Not all controls listed in ISO 27002 are suitable for every organisation. Different organisations have different organisational cultures and the cost of some controls may reduce their appropriateness for a particular organisation as well. Even more problematic is the situation where a new control interacts with existing controls. If there are inconsistencies in the security measures, or if a new control is not accepted by the employees of an organisation, there may be negative consequences for the effectiveness of existing controls as well.

As mentioned before, the current emphasis in Information Security standards is on the use of preventive controls. Hence, organisations may need to put in extra effort to identify detective controls in particular for those threats and/or vulnerabilities that are currently predominantly covered by preventive controls. It is common practice in information security to control a risk by implementing multiple overlapping controls. Hence, if a threat is serious enough to consider a preventive control, the security manager might want to consider a detective control as well. This detective control can either replace the preventive control (if a detection and response approach is cheaper) or it can be used to ensure that the organisation detects an attack that bypasses the preventive control.

Finally, similar to the discussions on the other artefacts in the previous sections, it is essential that there is a track record of which controls have been considered and which ones have been

rejected and why. Adequate documentation is essential when, after a serious incident, an organisation needs to evaluate its previous decisions on information security. And as situations change, controls that were previously considered inappropriate or too costly may have to be reconsidered when current security is no longer adequate.

Splitting Up the Monolithic Risk Assessment Process

The initial use of the artefacts produced by a risk assessment process is meant to be in the evaluation and selection of security controls, thereby allowing an organisation to assess the effectiveness of controls in covering its assets and the range of risks that it wants to protect them against. By emphasising these artefacts rather than the ranking of detailed risks, and by suggesting alternative processes to develop these artefacts, we are making a start in developing a new methodology. As these artefacts, however, have other, potentially more important, uses in security management (not just in risk assessment) the term security assessment methodology will be used in the rest of this paper instead of the term risk assessment methodology

The fundamental premise of this section is that a security assessment methodology will need to assist an organisation in identifying what needs to be protected as well as against who and for what aspect of security (confidentiality, integrity, etc). It will also need to identify current issues that most endanger organisational security and finally it will need to provide an insight into the most cost-effective way to achieve an adequate level of protection. Unfortunately, as discussed in previous sections, the current risk based information security approach is likely to be inadequate in each of these three areas. Notice that each of these aspects should influence the final prioritisation of security investments, but that the actual prioritisation itself is, in our view, a separate process.

Process 1: Ensuring the Identification and Security Classification of all Assets.

The first and, we believe, most critical area is the identification of assets and the categorisation of these assets according to what they need to be protected from (CIA, access, etc). While the term 'asset' is still used for now, this artefact should be extended to include systems, networks, information flows, business processes and knowledge. If management and employees in the organisation have no clear understanding what the organisation needs to protect, and from whom, good security is not achievable.

Identification and classification of assets will require significant effort from an organisation, but there is no need to produce this artefact in a single attempt: An iterative process is proposed instead. The organisation should start with identifying its major business process, and the systems, information flows and knowledge supporting this process. Gradually, over time, other business processes can be added and, every time an incident occurs, assets under threat should be identified. Social participation by all employees will offer an important contribution as well and will improve awareness at the same time.

To further improve the classification of assets the authors suggest the use of a consequence analysis based on Critical Impact Factors such as financial loss, loss of production, reputation damage and legal liability as proposed by Su *et al.* (2007). While this will undoubtedly increase the effort needed for, and slow down completion of, this process, the extra effort here will ensure that there will be better input data for the eventual decision making process on the prioritisation of security investments.

Process 2: Develop and Maintain an Extensive Threat and Vulnerability Database.

This aspect is similar to the creation of threat and vulnerability trees in risk assessment methodologies such as Octave. As in Octave, initial versions of these artefacts can be produced in a session of workshops, but after this initial phase maintenance and update of threat and vulnerability information becomes crucial.

While establishing a feedback process as part of incident handling is a necessary step, relying on current incident detection processes in an organisation may not be sufficient. Creating better situational awareness through the use of liaison officers in business units and extended implementation of detective controls will be necessary to significantly improve the quality of this threat and vulnerability information. In particular, the authors would like to see a systematic process of identifying threats and vulnerabilities that are currently not covered by detective controls, so the organization is aware which potential attacks may go undetected.

Process 3: Increase Knowledge on the Cost-effectiveness of Controls.

The final aspect is the need to build up knowledge within the organisation of controls and their cost-effectiveness. While there is a long list of controls in the current security standards, there is little in security literature on how effective these controls really are and which risks they cover. While organisations are often able to estimate the cost of implementing a particular control, the cost of maintaining that control can be much harder to budget. And when the maintenance cost slowly increases, this will often not be recognised. Knowledge about controls and their maintenance cost is essential when it is time to scale down security or to look for alternative controls. Hence, ensuring that organisations continue to extend their knowledge in this area is a worthwhile investment in security and allows the organisation to assess its current security posture.

A good example of the need for organisational memory in this area can be found in access control at the system level. While operating systems such as Windows have powerful access control capabilities, organisations will in general not use these capabilities. The cost of fine-tuning access control, and the cost of calls to the help desk when things go wrong, means most organisations prefer to avoid strict access control. Unfortunately they do not, in most cases, assess how much this open access policy costs the organisation by tracking the cost of incidents and the resulting forensic investigations. Even if they don't track incident costs, they should still consider whether the alternative use of detective controls (or honey pots) to identify user accounts that access sensitive documents would be cost-effective. A friendly chat with an employee, who has some abnormal access pattern, may prevent that employee from slowly extending his/her access to more sensitive documents, either out of curiosity or with malicious intent. Such a chat can sometimes also provide information indicating that an employee's user-account may have been compromised.

Process 4: Prioritization and balancing of controls

This process will use the output from the previous three processes to rank a set of controls. Again this should be an iterative process starting with a small set of controls that is currently being considered for implementation. When these controls are ranked according to how many (critical) assets are covered by each control, for which threats and vulnerabilities, and at what cost, additional controls may be added to this set for assessment.

It is important to realize that good security depends on achieving a reasonable balance between controls. It is normally not considered acceptable to invest heavily in one area of

information security and leave the organisation exposed in another area. Hence, ranking of controls should consider whether the current set of controls under consideration is not leaving the organisation exposed in other areas.

Similarly, there will need to be a balance between preventive controls and other controls, including incident response. Hence, the selection of potential controls, as well as the assessment of the cost-effectiveness of these controls, is complicated by the need to consider how to achieve, or maintain, this balance. As a result, prioritization will sometimes need to consider the optimum set of controls for a particular problem and rank this optimum set instead of just ranking each single control.

As security resources are limited, it is important that the prioritization of security investments also takes into account the current maintenance cost of security. As a result, it will become necessary to evaluate existing controls in this prioritization process. For instance, there obviously is an imbalance when an organization spends a significant amount of money on maintaining its firewall, but has no processes in place to assess and reduce the vulnerability of internal systems. In the current volatile security environment organisations will need to consider multiple overlapping controls including at least one detective control capable of identifying successful attacks that bypassed the preventive controls (Ruighaver, 2010). Hence, prioritization decisions may need to consider whether to reduce maintenance cost of one control to fund alternative overlapping controls.

Finally, it is important that realize that the quality of decision making on prioritisation may depend on how independent this process is from the previous three processes that collect the data used in this decision making. This might obviously be a problem in smaller organisations, where the number of employees in security management is limited, but even then the prioritisation should be the responsibility of a manager who is not directly involved in the previous three processes that provide the input to his/her decision making.

Potential Research Needed to Improve Security Assessment

Current security governance best practice suggests that a senior management committee should be made responsible for identifying the assets that need to be protected. There is no mention in literature, however, about how to prioritise these assets and who should be responsible for the prioritisation. Nor is there any indication of what business processes should be developed to support the asset identification and prioritisation.

Similarly, research on the effectiveness of the controls prescribed by current security standards is also lacking. For many of these controls it is not even clear which risks they are supposed to control. Again, the main problem for organisations is deciding where to start. Research on the prioritisation of controls, other than through the use of risk assessment, is urgently needed.

The extensive analysis of risk assessment artefacts and their use in security assessment in the previous section is based on the experience gained over the past decade through case study research in the areas of risk (Shedden *et al.*, 2006), security culture (Ruighaver *et al.*, 2007), and security governance (Tan *et al.*, 2005). Our challenge to the current use of traditional risk assessment, in particular, started as a result of our initial research in security culture (Chia *et al.*, 2003), which identified "The basis of truth and rationality" as one of the main dimensions of security culture. Over time, our continued investigation of this dimension has made us

critical of many of the underlying beliefs and assumptions used in current security management and security governance.

If we want to stop the current deterioration of information security in organisations, changing beliefs and attitudes of both management and employees, related to risks in particular and security in general, will need to be one of the most important areas of research in information security. This paper covers only one aspect of this enormous field as it attempts to change the beliefs of security professionals on the role of risk assessment in information security.

To provide an alternative to risk assessment in the selection of controls we suggested an approach that relies on the development of situational awareness in organisations. Over the past decade, situational awareness research has played an important role in safety but, until now, research on situational awareness in organisational information security has been confined to the area of network security.
Our research in security culture showed that most organisations lack internal focus (genuine interest in the security of information and its infrastructure) and instead have a purely external focus. Their main focus is often on the (partial) implementation of security standards to satisfy compliance requirements and to ensure they pass an eventual audit. As a result, we found these organisations have almost no situational awareness. We believe that a lack of knowledge in organisations on the classification of their assets, the extent of the current threats and vulnerabilities that are actually endangering these assets, and the effectiveness of the controls they have applied, is an important factor in the continuous growth of security incidents. Hence, research in these three areas is urgently needed.

However, to really change information security for the better, organisations will need to start treating information security as a strategic business problem. The term strategic is used here in the sense that organisations will need to build up a strategic security context (Tan *et al.*, 2005) with business objectives and business security strategies. Again this paper suggests the achievement of situational awareness as one objective and the use of detective controls and a security assessment methodology as potential strategies to achieve this goal.

Research in security as a business problem is just starting to take off. The economics of security has been getting more attention in literature recently (Gordon and Loeb, 2002), but research in actual business objectives for security and business strategy development is still lacking.

Conclusion

Information security is often considered to be a risk management problem and current security standards still advocate the use of risk assessment to guide an organisation's security planning. In a previous paper the authors reported on several case studies that examined how organisations actually perform a risk assessment. These case studies showed that in practice risk assessments are seldom used to select controls but are rather used to assist in audits, legislation compliance and transference of responsibility.

In this paper we have discussed the challenges in performing a systematic risk assessment at the organisational level and addressed some of the limitations of risk assessment for use in information security, even when that assessment follows the exact process described in the current risk management standard. The main value of traditional risk assessment outside the areas of compliance and transference of responsibility consists of the actual artefacts this process is supposed to produce.

The security assessment framework proposed in this paper identifies three processes that can be used to produce high quality versions of the artefacts used in traditional risk assessment. As the actual prioritization of security investments in the proposed security assessment framework does not depend on the extensive evaluation of individual risks for each critical asset, organisation's will be able to put more effort in asset classification, threat identification and/or control assessment to improve the quality of their decision making. Of course, traditional risk assessment may still have a role to play in the evaluation of residual risk, for legislation compliance and transference of responsibility, but that process should now also benefit from the improved quality of these artefacts.

Putting more emphasis on the artefacts produced by a risk assessment process and on the development of (business) processes to maintain and improve these artefacts extends their value for use in other areas of security management. While the security assessment methodology proposed in this paper will assist the organisation in achieving a better understanding of its assets and the security requirements for these assets, its main contribution to security management is the introduction of situational awareness as a business objective.

References

Alberts, C. and Dorofee, A. (2004). *Managing Information Security Risks*. Pittsburgh, Mellon Software Engineering Institute.

AS/NZS 4360. (1999). *'Risk management'*, Sydney, Australia/ Wellington, New Zealand. Standards Australia/ Standards New Zealand.

AS/NZS ISO/IEC 17799. (2001). *'Information technology – Code of practice for information security management'*, Sydney, Australia/ Wellington, New Zealand. Standards Australia/Standards New Zealand.

Chia, P., Maynard, S., and Ruighaver, A.B. (2003), 'Understanding Organisational Security Culture' in Hunter, M.G. and Dhanda, K.K. (eds), *Information Systems: The Challenges of Theory and Practice*, Information Institute, Las Vegas, USA, pages 335 - 365.

Coleman J. (2004). Assessing information security risk in healthcare organizations of different scale. In: Lemke HU, Vannier MW, Inamura K, Farman AG, Doi K, Reiber JHC (eds). *Proceedings of the 18th International Congress and Exhibition*, Computer Assisted Radiology and Surgery. Amsterdam: Elsevier, pp.125—130.

Endsley, M.R. (1995). Toward a Theory of Situation Awareness in Dynamic Systems. *Human Factors: The Journal of the Human Factors and Ergonomics Society,* 37 (1) , pp. 32- 64.

Gordon L.A., and Loeb M.P. (2002). 'The Economics of Information Security Investment', *ACM Transactions on Information and System Security*, Vol. 5, No. 4, November 2002, Pages 438-457.

Grant, T.J., Kooter, B.M., (2005). Comparing OODA & Other Models as Operational View C2 Architecture. *In: Proceedings of the 10th International Command and Control Research Technology Symposium*, McLean, VA.

HB 231. (2004). *'Information security risk management guidelines'*, Sydney, Australia/Wellington, New Zealand. Standards Australia/ Standards New Zealand.

Jaschob, A., Tsintsifa, L.: IT-Grundschutz. (2006). Two-Tier Risk Assessment for a Higher Efficiency in IT Security Management. In: Paulus, S., Pohlmann, N., and Reimer, H (ed) *Securing Electronic Business Processes*, pp 95--101.

Kailay, M.P., Jarratt P. (1995). RAMeX: a prototype expert system for computer security risk analysis and management. *Computers and Security*, Volume 14 Issue 5, pp. 449-463.

Norman P.M., (2001), 'Are your Secrets Safe? Knowledge Protection in Strategic Alliances', *Business Horizons*, Vol 44(6) pp 51-60.

PITAC. (2005). Cyber Security: A crisis of prioritization – report to the president. Technical report, President's Information Technology Advisory Committee.

Ruighaver, A.B., Maynard, S., and Chang, S. (2007), 'Organizational Security Culture: Extending the End-User Perspective', *Computers & Security*, Volume 26, Issue 1, February 2007, Pages 56-62.

Ruighaver A.B. (2010). Organisational security requirements: An agile approach to Ubiquitous Information Security, *Journal of Information warfare,* Volume 9, Issue 1.

Sasse, M.A., Brostoff, S. and Weirich, D. (2001). Transforming the "weakest link": a human-computer interaction approach to usable and effective security. *BT Technical Journal*, Vol 19 (3) July 2001, pp. 122-131.

Shedden, P., Ruighaver, A.B., Ahmad, A. (2006). Risk Management Standards – The Perception of Ease of Use. *5th Security Conference*, April 19-20 2006 Las Vegas, USA.

Su, X., Bolzoni, D., and van Eck, P. (2007). Understanding and Specifying Information Security Needs to Support the Delivery of High Quality Security Services. In: Int. Conference on Emerging Security Information, Systems and Technologies, pp. 107-114.

Tan, T. and Ruighaver A.B. (2005). Understanding the scope of strategic context in security governance, In B Cusack (ed), *IT Audit: A Strategic Foundation for Corporate Governance*, 65-77. Auckland, New Zealand: School of Computer & Information Science, Auckland University of Technology.

Whitman, M.E. and Mattord, H.J. (2005). *Principles of Information Security*, Thomson Course Technology, United States of America.

Wipawayangkool, K. (2009) Security Awareness and Security Training: An Attitudinal Perspective," *Proceedings of the 40th Southwest Decision Sciences Annual Conference*, Oklahoma City, OK, USA, February 25-28, pp. 266-273.

Visintine, V. (2003). *An Introduction to Information Risk Assessment*, SANS Institute.