APPLYING THE AUSTRALIAN AND NEW ZEALAND RISK MANAGEMENT STANDARD TO INFORMATION SYSTEMS IN SMES

Robyn A Davidson,
PhD student, School of Commerce,
The Flinders University of South Australia,
GPO Box 2100,
Adelaide South Australia 5001.
Telephone: +61 8 82013081
Facsimile: +61 8 82012644
Email: Robyn.Davidson@flinders.edu.au

Susan C Lambert,
Lecturer, School of Commerce,
The Flinders University of South Australia,
GPO Box 2100,
Adelaide South Australia 5001.
Telephone: +61 8 82012766
Facsimile: +61 8 82012644
Email: Susan.Lambert@flinders.edu.au
Nominated author for correspondence: Robyn Davidson

ABSTRACT

This paper advocates the use of the Australia/New Zealand Risk Management Standard (SA/SNZ, 1999) in conjunction with of a modified version of Birch and McEvoy's (1992) Structured Risk Analysis for Information Systems (SRA-IS) to identify information systems security risks in SMEs. The use of Internet based commerce by SMEs exposes them to information systems security risks that they are ill equipped to recognise let alone mitigate. Unlike the identification of some business risks, identification of risks associated with information systems requires certain technical expertise. The structure of the existing information system must be understood and modelled before risks can be identified and it is acknowledged that the required technical expertise may not be present in SMEs, thus the involvement of information systems consultants may be necessary. Once the information system has been modelled little information systems expertise is required to complete the analysis, keeping consultant involvement to a minimum and maximising owner/manager involvement.

INTRODUCTION

Small and Medium Enterprise (SME) owner/managers recognise and deal with risks in many aspects of their business. Risk in relation to destruction or theft of physical assets, theft or unauthorised use of intellectual property, financial risk associated with undertaking large contracts. "The need to manage risk systematically applies to all organisations and to all functions and activities within an organisation and should be recognised as of fundamental importance by all managers and staff" (Knight, 1999). One such function is the provision of information systems. Information is the lifeblood of any business. Turn off the information system for a day and chances are productivity will come to a grinding halt. Similar consequences will result from the system working ineffectively or from the integrity of data being compromised.

The increasing use of networked information systems within SMEs can be the source of serious security problems (Spinellis, Kokolakis & Gritzalis, 1999). The fact that the business is small does not mean that it will escape the notice of would be hackers. "Hackers normally do not attack sites based on the profile of companies, but randomly target a range of Internet protocol addresses and seek to infiltrate on a sequential basis…" (See cited in Ravendran, 2001). SMEs need to understand that once connected to the Internet they are equally at risk of attack as any other organisation. Giannacopoulos (2002) states that, "Somewhere, sometime, someone will target your company for attack...".

SMEs typically lack the technical expertise and resources to effectively identify and manage risk (Spinellis *et al,* 1999). Many SMEs are unaware of the risks that face their information systems so it is hardly surprising that they do not take adequate security measures. What is needed is a method

that can be applied by SME owner/managers to identify risks and measure them so that appropriate risk management decisions can be made. This paper shows how the Australia/New Zealand Standard: Risk Management (SA/SNZ, 1999) can be used by SME owner/managers to identify and evaluate risks.

The Australian/New Zealand Standard: Risk Management (SA/SNZ, 1999) defines risk as "the chance of something happening that will have an impact upon objectives". The risk materialises when a threat such as a hardware failure, data being tampered with or the system being destroyed by fire, is coupled with a vulnerability such as unrestricted access to premises. Threats to information systems (IS) can arise from accidental errors or mishaps such as power failures, accidental equipment breakage or equipment failure. Threats can also arise from criminal attacks such as spying by competitors, impersonation to gather information or steal from users, denial of service attacks or malicious content attacks.

These threats can come from inside or from outside the organisation, they may be intentional or unintentional but whatever the cause, the damage can be avoided or at least reduced by applying a methodical risk management plan and process.

RISK MANAGEMENT AND THE SECURITY POLICY

Risk management begins with the development of a security policy that defines how risks will be identified, analysed, evaluated and treated. It should be an organisation wide policy that covers all aspects of the business. To this end the organisation needs to be divided into appropriate units for risk consideration such as customer relations, occupational health and safety, production, inventory and information systems. The security policy should clearly define what is to be secured, why it needs to be secured, and how it is to be secured. The intention of the policy is not to give the technical details of how security will actually be achieved but to state how the risk management process will be implemented. The technical aspects of how security will actually be achieved will depend on what risks and treatment options are identified and the cost of these options.

The Australia / New Zealand Standard: Risk Management (SA/SNZ, 1999) provides a "generic guide for the establishment and implementation of a risk management process". This standard can be applied to a wide range of organisations for a number of applications, including risk management of information systems. The risk management standard provides a:

"logical and systematic method of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risks associated with any activity, function or process in a way that will enable organisations to minimise losses and maximise opportunities" (SA/SNZ, 1999, p.1).

The process is illustrated in Figure 1 and discussion of each stage follows. It is important that all assumptions, methods, data sources and results of the risk management process be carefully and thoroughly documented. The documentation will provide evidence of a systematic approach to risk identification and analysis, as well as forming the basis of a knowledge database of the recorded risks to the organisation. The documentation will also provide decision-makers with a basis for their decisions and will facilitate ongoing review, and communication of the information to stakeholders (SA/SNZ, 1999, p.21).

The standard recommends that a structured method for risk identification and assessment be used but falls short of providing such a process. The problem SMEs find with risk assessment methods for information systems is that they are difficult to administer because they require technical expertise that is not present in house. The process often needs to be outsourced which means considerable expense. What the authors of this paper have endeavoured to design is a method that isolates the technical, information systems tasks and provides a technique for owner/managers to apply to their own information systems. The process recommended in this paper is a simplified version of Birch and McEvoy's (1992) Structured Risk Analysis for Information Systems Method (SRA-IS). In Figure 1, the Australian/New Zealand Standard Risk Management Process has been divided into five phases and SRA-IS has been mapped onto each phase to show how it can be applied to each task.

Phase 1: Establish the context in which the Risk Management Process will take place

Establishing the context involves defining the strategic context, the organisational context and the risk management context in which the risk management process (RMP) will take place. Criteria against which risks will be evaluated and the structure of the analysis should also be defined at this stage (SA/SNZ, 1999, p.7).

The *strategic context* provides a description of the organisation; where it sits within the industry, who controls it, who its customers are, how big it is, its employee profile and the major strengths, weaknesses, threats and opportunities that face the organisation (SA/SNZ, 1999, p.9).

The *organisational context* refers to "the capabilities, goals and objectives of the organisation and the strategies that are in place to achieve them" (SA/SNZ, 1999, p.9). The organisational context in which the RMP is to be implemented must be defined and understood so that the RMP can be designed to complement, or at least not conflict with, organisational goals and objectives.

The *risk management context* refers to establishing the "goals, objectives, strategies, scope and parameters of the activity, or part of the organisation to which the RMP is being applied" (SA/SNZ, 1999, p.10). Determining the risk management context requires the definition of a "risk unit(s)" or part of the organisation or that function of the organisation to which the RMP is to be applied. The risk units of an organisation might include occupational health and safety, warehousing, property management or information systems. Several RMPs might exist in a single organisation making up the over-all RMP of the entire organisation.

Criteria against which risks are evaluated need to be determined (This relates to Phase 4: Evaluate Risks). This enables the users to identify risks that are acceptable and those that are not acceptable. If the risk falls outside the acceptable range action needs to be taken to reduce the risk. It is up to the users to set the level of risk that they are willing to accept and the level that they cannot accept. For instance, users might decide to measure risks on a qualitative scale of "Low" to "Extreme" and that risks with a value of "High" or "Extreme" are not acceptable. Risks that fall into the "High" or "Extreme" categories require immediate treatments to bring them down to at least the "Moderate" level. The criteria used will depend on the method used to measure risks. This is discussed in Phase 3: Analyse Risks.

A *structured* method is needed to systematically identify all risks. In this phase, the structure to be used should be decided upon and documented. Structured analysis techniques are discussed in Phase 2: Identify Risks.

Phase 2: Identify risks

The aim of the risk identification stage is to generate a comprehensive list of all risks facing the organisational unit regardless of whether they are or are not under the control of the organisation. It is essential that a well-structured process be used, so that all significant risks are identified; if they are not identified at this stage they are excluded from analysis. (SA/SNZ, 1999, p.12).

How can we be confident that all risks have been identified? Certainly, something more than intuition and brainstorming is required. A properly applied *structured* analysis technique will ensures all risks are identified. This involves separating the activity into a set of elements, which provides a logical framework for identification and analysis (SA/SNZ, 1999, p.12). Many structured analysis techniques have been developed. Examples of these are the COBRA Risk Consultant (C & A Systems Security, 2002), CRAMM (Gamma Secure Systems, 2002), and Structured Risk Analysis for Information Systems (Birch & McEvoy, 1992) methods. These methods typically have a structured way of capturing all of the information necessary to support risk analysis that allows all risks to be identified and analysed. Birch and McEvoy's Structured Risk Analysis for Information Systems (SRA-IS) method is adopted in this paper.

All structured techniques require considerable skills from the users. This is a draw back for smaller organisations since it often requires extensive use of expert information systems security consultants, which translates to a prohibitively expensive exercise. The SRA-IS technique is no exception, however, the adaptations proposed in this paper require minimal technical expertise to implement. SRA-IS requires the organisation to build three models from which threats,

vulnerabilities and ultimately risks are derived. It is vital that these models accurately reflect the information assets, physical assets and the information flows and stores of the organisation. It is in building these models that technical skills are required. This is the only stage that requires specialist information systems skills and since it is such a vital stage of the process, it is recommended that the skills be outsourced if they do not exist within the organisation. The application of the models requires general business skills and knowledge of the business, skills that are likely to exist within the business. The models upon which all risks are derived are the information model (from which threats are derived), the technology model (from which vulnerabilities are derived) and the business model that links the information and technology models.

Risks are the manifestation of threats and vulnerabilities. It is useful then to identify threats and vulnerabilities and derive risks from these. A threat is something that will have an adverse effect on an organisation and exists whether or not there are any practical or apparent ways in which it might ever be manifested. Threats to information systems can be divided into three categories as shown in Table 1.

Birch and McEvoy (1992) define a vulnerability as a characteristic of a physical system, which allows a threat to be exploited, while being independent from any specific threat. IS vulnerabilities are categorised by the type of threat to which they relate as shown in Table 2.

Figure 1: Risk Management Process

Source: Adapted from SA/SNZ, 1999, p.11

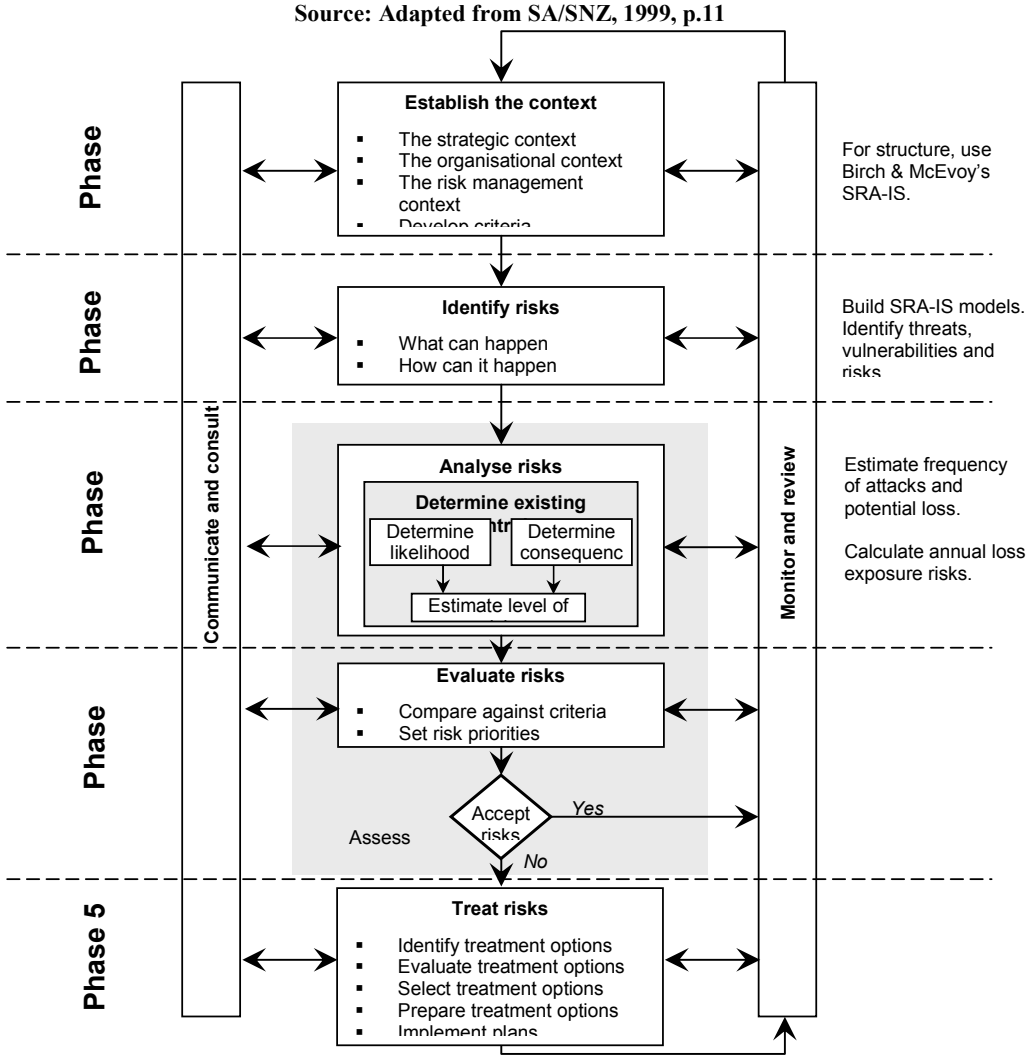


Table 1: Types of Threats

Threat Category	Explanation
Those that threaten data **confidentiality**	Private and sensitive data must be kept confidential.
Those that threaten data/system **integrity**	Data and programs should only be changed by authorised personnel.
Those that threaten data/system a**vailability**	The IS should operate effectively and efficiently to ensure service to authorised users.

Table 2: Types of Vulnerabilities

Threat	Vulnerability
Threats relating to data **confidentiality** can be exploited if…	physical assets and communication links can be **accessed** by unauthorised personnel.
Threats to data/system **integrity** can be exploited if….	physical assets and communication links can be **tampered** with.
Threats to data/system **availability** can be exploited if…	physical assets and communication links can be **damaged**.

Table 3 shows some possible vulnerabilities to a telephone line communication link and the threats to the data that travels through the line.

Table 3: An Example of Vulnerabilities and Threats

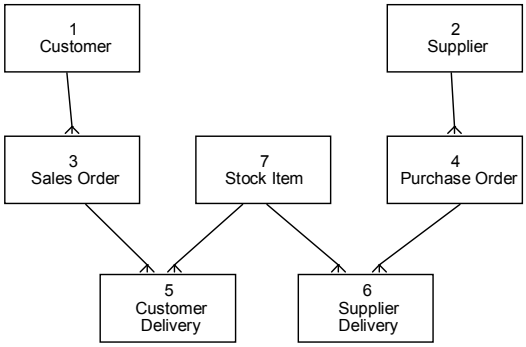
Vulnerability relating to the communication link "telephone line"	**Threat relating to the information asset "data"**
The telephone line may be **accessed** by using a wire-tap.	Data is viewed by unauthorised parties. Loss of **confidentiality** of data.
The telephone line may be **tampered** with by being redirected.	Data is lost or corrupted. Data **integrity** is lost.
The telephone line could be **damaged** by being cut.	The system is inaccessible. Data is **unavailable**.

By cross-referencing the identified threats (what can happen to the information asset) with the identified vulnerabilities (how it can happen) a complete list of risks can be identified. An organisation is therefore at risk when there is a threat to the business and a vulnerability that may be exploited to realise that threat. Once a complete list of risks has been identified they are analysed.

Information Model

Identifying the threats using the Birch and McEvoy (1992) method requires the user to build an "Information Model" that identifies all of the information assets of the organisation, i.e. all of the elements of the organisation about which information is generated. These elements include customers, suppliers, and transactions such as sales and deliveries and details of the goods and services traded by the organisation. A simple information model for a retail organisation is shown in Figure 2. Each information asset maybe subject to an integrity threat (I), a confidentiality threat (C), or an accessibility threat (A). Each threat identified in the information model is catalogued in a table such as that shown in Table 4 along with an estimate of the loss the business would suffer should the threat be realised. The loss estimate figure will depend on the type of analysis used. See Phase 3: Analysis.

Figure 2: Information Model Example



Source: Birch & McEvoy, 1992

Table 4: Threat Catalogue Extract

Inf. Asset	Information Asset Name	Threat ID	Description of Threat to Information Asset	Loss (L)
1	Customer	I1	Customer Lost/corrupt	3
	Customer	C1	Customer Disclosed	3
	Customer	A1	Customer Not Available	2
2	Supplier	I2	Supplier Lost/corrupt	4
	Supplier	C2	Supplier Disclosed	4
	Supplier	A2	Supplier Not Available	3
3	Sales Order	I3	Sales Order Lost/corrupt	2
	Sales Order	C3	Sales Order Disclosed	2
	Sales Order	A3	Sales Order Not Available	1
4	Purchase Order	I4	Purchase Order Lost/corrupt	1
	Purchase Order	C4	Purchase Order Disclosed	1
	Purchase Order	A4	Purchase Order Not Available	2

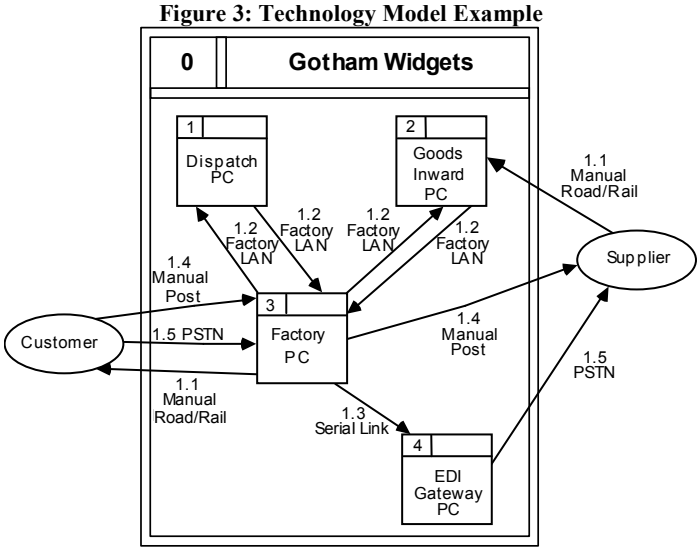
Source: Adapted from Birch & McEvoy, 1992

"Customer" data from Figure 2 is the "customer information asset 1" in Table 4, "supplier" data from Figure 2 is the "supplier information asset 2" in Table 4, etc. Table 4 shows that for every information asset there are three potential threats, e.g. there may be a threat to customer data integrity (I1), customer data confidentiality (C1), or access to customer data (A1).

Technology Model

The technology model identifies the physical information system assets of the organisation such as file servers, Internet connections, personal computers, and local area networks (LANs). A simple technology model relating to a retail organisation is shown in Figure 3.

Figure 3: Technology Model Example



Source: Birch & McEvoy, 1992

Figure 3 shows four personal computers (PCs) connected by a local area network (LAN). Customers and suppliers can provide or get information by telephone (public switched telephone network – PSTN), through the post, or with deliveries by road or rail. It is from these physical assets that vulnerabilities can be derived. Each physical asset may be vulnerable to unauthorised access, tampering or damage. Unauthorised access can threaten data confidentiality. Tampering can threaten data and system integrity. Damage to physical assets can restrict or prevent access to data and the system. Each vulnerability is catalogued in a table such as that shown in Table 5 along with an estimate of the frequency of the vulnerability being exploited. The frequency estimate, like the loss estimate, depends on the type of analysis used. See Phase 3: Analysis.

Table 5: Vulnerability Catalogue Extract

Phy. Asset	Physical Asset Name	Vul. ID	Description of Vulnerability of Physical Asset	Prob (P)
1	Dispatch PC	I1	Dispatch PC Tampered	-2
	Dispatch PC	C1	Dispatch PC Accessed	0
	Dispatch PC	A1	Dispatch PC Damaged	-1
2	Goods In PC	I2	Goods In PC Tampered	-2
	Goods In PC	C2	Goods In PC Accessed	0
	Goods In PC	A2	Goods In PC Damaged	-1
3	Factory PC	I3	Factory PC Tampered	-3
	Factory PC	C3	Factory PC Accessed	-1
	Factory PC	A3	Factory PC Damaged	-2
4	EDI Gateway PC	I4	EDI Gateway PC Tampered	-2
	EDI Gateway PC	C4	EDI Gateway PC Accessed	0
	EDI Gateway PC	A4	EDI Gateway PC Damaged	-1
1.1	Road/Rail	I1.1	Road/Rail Tampered	-2
	Road/Rail	C1.1	Road/Rail Accessed	0
	Road/Rail	A1.1	Road/Rail Damaged	-1

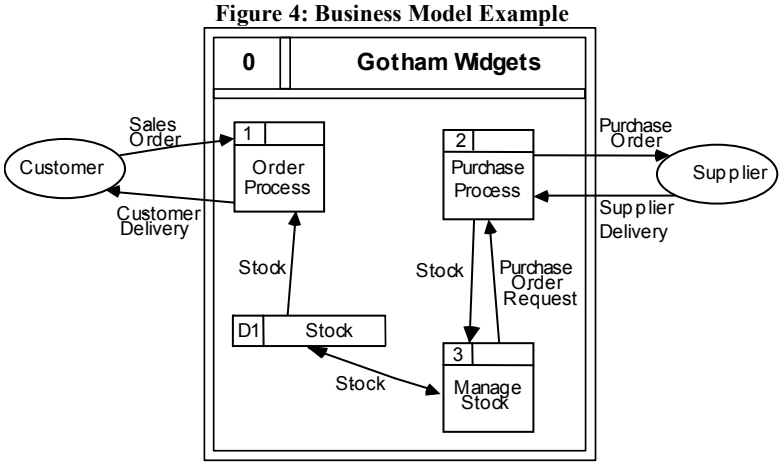
Source: Adapted from Birch & McEvoy, 1992

Business Model

The next step is to determine the vulnerabilities that might cause a threat to be realised. For instance, access to customer order information will be threatened if the file server holding that data is damaged. If the organisation operates over the Internet then the same threat could be realised if

the telephone line connecting the file server to the Internet is damaged. A methodical structured process is required to ensure all vulnerabilities are matched to each threat. It is the business model that provides the required link between the information model (threats) and the technology model (vulnerabilities). The business model is used to expose risks by linking the threats identified from the information model and the vulnerabilities identified from the technology model. The business model shows the flows, sources and sinks of information, along with the information processing and retention centres (Birch & McEvoy, 1992). Figure 4 shows a simple retail business model.

Figure 4: Business Model Example



Source: Adapted from Birch & McEvoy 1992

In Figure 4, the "customer" and "supplier" are external entities that provide (source) and receive (sink) data through the data flows indicated by the arrows. This is data about the sales order, customer delivery, purchase order, and supplier delivery. The square boxes represent processes that transform data. A process transforms the data in some way, such as updating stock levels, and sends the data to another process or to a data store. A data store is represented by a rectangle.

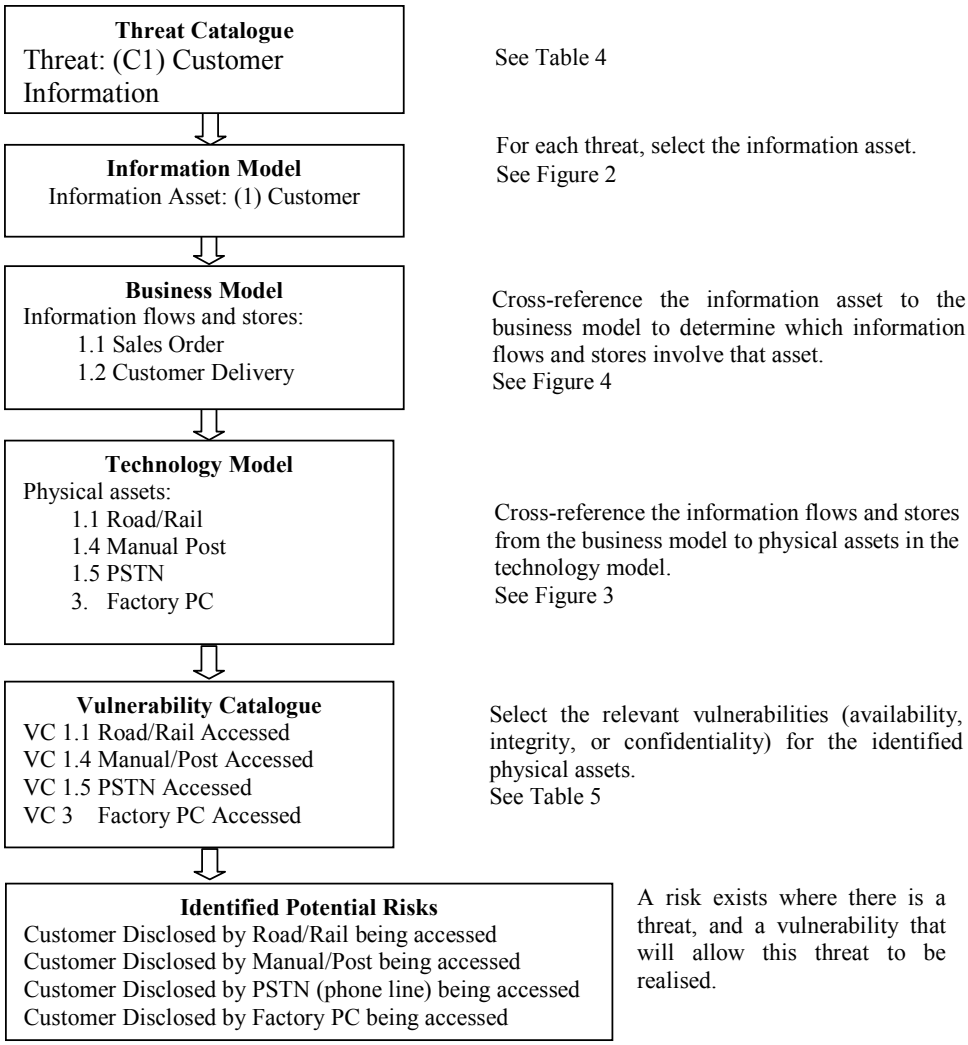
Coding of information assets, physical assets, and each element of the business model allows for cross-referencing and ultimately matching of vulnerabilities and threats and therefore risks. An example of how to determine the risks for the threat that customer information may be disclosed is illustrated in Figure 5.

This can be a tedious and error prone exercise but can be automated with the use of a database program. Davidson (2000a; 2000b) developed a program that was tested on the information systems of small public accounting practices and it proved to be a successful method to determine risks. The elements of each model and the relationships between these elements are input into the program. Every threat (lost/corrupt, disclosed, not available) and vulnerability (damaged, accessed, tampered) is then automatically generated. Using the inputted loss and frequency estimates the program generates a complete list of risks with calculated loss exposure figures.

Phase 3: Analyse risks

In order to assess the significance of a potential risk each risk must be assigned a value. For each potential risk, an estimate must be made of the resulting consequences or loss should the threat be realised and an estimate of the likelihood or frequency of the vulnerability being exploited. Estimates can be made based on historical evidence and from the judgements of personnel with knowledge of the relevant threats and vulnerabilities. The estimates can be quantitative, semi-quantitative or qualitative (SA/SNZ, 1999, p.13).

Figure 5: Cross Referencing Between Models to Determine Risks



Quantitative estimates are particularly useful when consequences can be expressed in dollar terms, and likelihood can be expressed as frequency per year. The risk level is then expressed as an annual loss exposure (ALE) in 'dollars per year'. The advantage of quantitative analysis is that it facilitates cost-benefit analysis and can help justify expenditure. However, any inaccuracy in estimates can lead to wildly inaccurate ALE figures (Dorey, 1991).

Qualitative estimates use descriptive terms. Consequences can be measured on a scale such as "low to huge" financial loss and likelihood of the event occurring can be expressed as "rare to almost certain". Qualitative estimates are appropriate in situations where it is difficult to accurately estimate losses. A matrix is used to combine the consequences and losses resulting in a loss exposure of "low" to "extreme" (Dorey, 1991; (SA/SNZ, 1999, p.14 & 34-35).

Semi-quantitative analysis gives numerical values to qualitative scales. This allows numerical values to be combined to produce a numerical risk level. The risk level does not represent an

intrinsic value such as that produced in quantitative analysis. Semi-quantitative analysis has the advantage of allowing subjective assessments but ranks risks in more detail than achieved with qualitative analysis (Dorey, 1991).
Birch and McEvoy's (1992) SRA-IS method uses a semi-quantitative analysis which produces a detailed ranked list of risks. Semi-quantitative analysis is appropriate where it is difficult to estimate intangible losses such as loss of reputation, loss of client data, and sales histories, but a more detailed ranking of risks is required than that provided by qualitative analysis.

Phase 4: Evaluate risks

This stage of the RMP compares the level of risk found during the analysis process with the risk evaluation criteria established in the "Establish the Context" stage discussed in Phase 1 (SA/SNZ, 1999, p.15).
An organisation using qualitative analysis may establish that "extreme" and "high" risks require immediate attention, "low" risks are acceptable and "moderate" risks will be considered on a case by case basis to determine their level of acceptability. An organisation using quantitative analysis can set levels of acceptability in numerical terms such as, risks with an ALE of "x dollars per year" or less are acceptable. Any risk with an ALE in excess of "x dollars per year" requires immediate attention.
Semi-quantitative analysis allows an acceptable level of risk to be set similar to quantitative analysis. However, the figure does not represent a dollar value per year, but indicates the seriousness of the risk relative to the other risks. For instance, a risk with an exposure of 4 is more serious than a risk with an exposure of 3.
Appropriate treatment must be determined for those risks that are deemed unacceptable, whilst those risks determined to be acceptable should be monitored and periodically reviewed to ensure that they remain acceptable.

Phase 5: Treat risks

There are three steps in treating risks:
Step 1. Identify treatment options;
Step 2. Evaluate and select treatment options; and
Step 3. Prepare and implement treatment plans.

Step 1: Identify Treatment Options
Five treatment options are available:

1. avoid the risk;
2. reduce the likelihood of the occurrence;
3. reduce the consequences;
4. transfer the risk; or
5. retain the risk (SA/SNZ, 1999, p.16).

Risk avoidance involves eliminating the activities that generated the risk. For example, being connected to the Internet poses a risk that an attacker could access sensitive files. This risk can be avoided by simply disconnecting from the Internet. Care must be taken however to ensure that the risk avoidance measures do not conflict with the strategic objectives of the organisation identified in Phase 1. This requires the analyst to consider both the costs and benefits of applying the treatment.
The likelihood of the risk occurring relates to the vulnerabilities of the IS. Therefore, to *reduce the likelihood of an occurrence,* the vulnerabilities can be treated so that the expected frequency of an attack falls to a level that generates an acceptable risk level. For instance, the risk of an outside party tapping into the customer data could be reduced through the use of a firewall to restrict access.
The consequences, should the threat be realised, refer to the economic or other loss experienced should an attack take place. Thus *consequences can be reduced* in many ways such as daily backups

of all files, or minimising the number of files stored on the computer that is connected to the Internet.
Another way of reducing the loss or consequence of an attack is by *transferring* part or all of the loss to a third party through insurance. This is not always appropriate for IS risks since often the damage to or loss of data cannot be monetarily compensated.
Retaining the risk is another option. Individual risk profiles differ; therefore, some organisations will retain more risks than others. After treating risks to reduce them there will be residual risks or new risks arising from treatment. It is important that users revisit their original criteria to ensure they are comfortable with the levels in terms of both costs and benefits.

Step 2: Evaluate and Select Treatment Options

The risk treatment options must be assessed in terms of the effect they will have on the organisation and the cost of implementing them. The benefits obtained from implementing the treatment options should outweigh the costs (both monetary and non-monetary). Identifying appropriate treatment options requires both business and technical IS skills and knowledge. Treatment options can be aimed at decreasing the impact rating of the threat, i.e. decreasing the loss should an attack occur. For example, by backing up data twice daily so that if the hard drive crashes during the day only half a day's data needs to be reconstructed. Alternatively, the treatment option might be aimed at reducing the vulnerability by decreasing the likelihood of the physical item being accessed, tampered with or damaged. For example, by placing all telecommunication cables underground to decrease the likelihood of them being cut by vandals. The best options are those where large reductions can be obtained with relatively low expenditure. There may be cases of rare severe risks that will warrant treatment that cannot be justified on economic grounds alone, these cases need to be considered on a case-by-case basis.
The Australian/New Zealand Standard: Information Security Management (SA/SNZ, 2000) provides a list of control objectives and the related controls that can be applied to suit the needs of various organisations.

Step 3. Prepare and Implement Treatment Plans

The risk treatment plan documents the controls that have been chosen to treat the risks. It also states who has responsibility for implementing the plan, what resources are to be utilised, budget allocation and the timetable for implementation. The plan will also include details of how compliance with the treatment plan will be reviewed (SA/SNZ, 1999, p.41).

MONITORING AND REVIEW

Monitoring and reviewing, as shown in Figure 1, is an ongoing process that is part of every stage of the complete RMP. As well as monitoring the effectiveness of the risk treatment plan and how it was implemented, risks and their control measures need to be continually monitored, as few risks remain static. Circumstances can change which affect the likelihood and consequences of an event, as well as the suitability of treatment options. By regularly repeating the risk management cycle it ensures that the management of risks remains relevant (SA/SNZ, 1999, p.20).

COMMUNICATION AND CONSULTATION

Throughout the RMP various stakeholders should be consulted and kept informed of findings and proposed actions. The stakeholders are those who can be affected by a decision or activity and include employees, management, insurance organisations, financiers, customers and suppliers.

RISK MANAGEMENT SUMMARY

The Australian/New Zealand Standard: Risk Management (SA/SNZ, 1999) describes a standard procedure for managing risks. This procedure takes the form of iterating through the five phases of establishing the context, identifying, analysing, evaluating, and treating risks. Throughout these five phases there is continual monitoring and review of the processes and the stakeholders are communicated with and consulted. This is a generic procedure that can be applied to a wide range of organisations and activities.

When implementing the RMP the risk assessor needs to have a good knowledge of the organisation and types of threats and vulnerabilities it faces to be able to identify, analyse and evaluate risks. The risk assessor needs to be able to accurately break the information structure down into elements in order to identify systematically all threats and vulnerabilities. Recognition of the value of the information is crucial to enable accurate estimates of the loss that would arise should a threat be realised. Similarly, historical evidence and good judgement is essential to accurately estimate the likelihood of vulnerabilities being exploited.

The example given in this paper uses a simplified version of Birch and McEvoy's (1992) SRA-IS method. A more complex version systematically derives all risks and vulnerabilities from models of the organisation's information system. It calculates an exposure level taking into account:

- the loss to the organisation and gain to an attacker should a threat be realised,
- the frequency of exploiting a vulnerability and the cost to an attacker to do so, and
- the four different types of attackers.

Davidson (2000a) has written a computerised risk analysis program based on this method. This program simplifies the RMP by automating the generation of threats, vulnerabilities, risks and exposure levels. The risk assessor must also have a good knowledge of what risk treatment options are available.

CONCLUSION

Information system security is a serious concern to SMEs operating in networked information systems environments. Before owner/managers can implement appropriate security measures however they must identify and evaluate the risks that they face. This paper has provided a method of identifying and evaluating information system security risks that is consistent with the recommendations of the Australian/New Zealand Standard: Risk Management (SA/SNZ, 1999). The application of this structured risk analysis technique can be supported by a purpose built database. This, like any other information systems analysis does require accurate systems modelling, the skills for which may need to be outsourced. This should not be looked upon as a major obstacle but as the foundation of future systems security management.

Ignoring information system security could result in irrecoverable damage to the tangible and/or intangible assets of the business. Applying ad hoc security measures may result in the misdirection of resources. A systematic approach to risk management will provide owner/managers with the information needed to make cost justified information systems security decisions. Resources can then be allocated in a way that maximises the benefits to the organisation.

REFERENCES

Birch, D. G. W., & McEvoy, N. A., 1992, 'Risk Analysis for Information Systems', **Journal of Information Technology,** vol. 7, pp. 44-53.

C & A Systems Security Ltd, 2002, 'Introduction to Security Risk Analysis and the COBRA Approach', available on-line from http://www.securitypolicy.co.uk/risk analysis/, last accessed 1/7/02.

Davidson, R. A., 2000a, 'Information Systems Risk Analysis Method', computer program, available by contacting Robyn.Davidson@flinders.edu.au.

Davidson, R. A., 2000b, 'Information Systems Risk Analysis for Smaller South Australian Public Accounting Practices', Honours Thesis, School of Commerce, Flinders University of South Australia.

Dorey, P. G., 1991, 'Risk Assessment - Current Methodologies and Software Products', **Information Security Monitor,** vol. 7, no. 1, pp. 5-7.

Gamma Secure Systems, 2002, 'A Practitioner's view of CRAMM', available on-line from http://www.gammass1.co.uk/topics/hot5.html, last accessed 28/6/02.

Giannacopoulos, P., 2002, 'Paranoia is Good', **Strategic Finance**, Montvale, vol. 83, no. 8, pp. 26-29.

Knight, K., 1999, **A Basic Introduction to Managing Risk, (HB 142-1999),** Standards Association of Australia.

Ravendran, A., 2001, 'Low Security Awareness Among SMEs', **Computimes Malaysia**, New York, August 30.

Spinellis, D., Kokolakis, S. & Gritzalis, S., 1999, 'Security Requirements, Risks and Recommendations for Small Enterprise and Home-office Environment'**, Information Management & Computer Security**, vol. 7, no. 3, pp. 121-128.

Standards Australia & Standards New Zealand (SA/SNZ) 1999, **AS/NZS 4360:1999 Risk Management,** Standards Australia & Standards New Zealand, Homebush, Aust., Wellington, NZ.

Standards Australia & Standards New Zealand (SA/SNZ) 2000, **AS/NZS 7799.2:2000 Information Security Management,** Standards Australia & Standards New Zealand, Homebush, Aust., Wellington, NZ.