CIIP-RAM - A SECURITY RISK ANALYSIS METHODOLOGY FOR CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

T. B. Busuttil[1], and M. J. Warren[2]
[1] *School of Information Technology, Deakin University, Australia;* [2]*School of Information Systems, Deakin University, Australia*
{tbb; mwarren}@deakin.edu.au

Abstract: Critical Information Infrastructure has become a priority for all levels of management, It is one of the key components of efficient business and business continuity plans. There is a need for a new security methodology to deal with the new and unique attack threats and vulnerabilities associated with the new information technology security paradigm. CIIP-RAM, is a new security risk analysis method which copes with the shift from computer/information security to critical information infrastructure protection. This type of methodology is the next step toward handling information technology security risk at all levels from upper management information security down to firewall configurations. The paper will present the methodology of the new techniques and their application to critical information infrastructure protection. The associated advantages of this methodology will also be discussed.

Key words: Critical Information Infrastructure, Security Risk Analysis and Information Security.

1. INTRODUCTION

Understanding and managing Critical Information Infrastructure (CII) security risks is a priority to most organisations dealing with Information Technology (IT) and Information Warfare (IW) scenarios today (Libicki 2000). Traditional security risk analysis was well suited to these tasks within the paradigm of computer security where the focus was on securing tangible items such as computing and

communications equipment (NCS 1996, Cramer 1998). With the growth of information interchange and reliance on information infrastructure, the ability to understand where vulnerabilities lie within an organisation, regardless of size, has become extremely difficult (NIPC 1996). To place a value on the information that is owned and used by an organisation is virtually an impossible task (Busuttil and Warren 2001a). The suitability of risk analysis to assist in managing Critical Information Infrastructure-related security risks is unqualified, however studies have been undertaken to build frameworks and methodologies for modelling Information Attacks (Beer 1984, Molander et al. 1996, Johnson 1997, Busuttil and Warren 2001b, Hutchinson and Warren 2001) which will assist greatly in applying risk analysis concepts and methodologies to the burgeoning information technology security paradigm, Information Warfare. The concept of behind this unique method of security risk analysis takes the form of the conceptual model of layered logical transformation models (LTMs) (Busuttil and Warren 2002). These models allow stakeholders to apply risk analysis to traditional IW scenarios so as to deal with the problems of scalability and inaccurate cost analysis as well as being dynamic enough to keep up with the constant changes occurring in information infrastructure and information attacks.

2. A NEW METHOD OF SECURITY RISK ANALYSIS AND INFORMATION INFRASTRUCTURE PROTECTION

Third generation security risk analysis methodologies, LTMs, were designed to work well when built into information system security risk analysis scenarios from the beginning (Baskerville 1993). The major characteristics of IW and CII Protection which set them apart from information security (IS) are the need to take (1) organisational scalability, (2) flexibility and (3) difficulty in cost evaluating of threats, vulnerabilities and attacks into account when considering CII Issues. So to adapt LTM security risk analysis technology from IS to CII protection these issues of scalability and adaptability must first be dealt with.

One of the major advantages of LTMs are the ability to build security into information systems in an adaptable manner (Baskerville 1993). The flexibility of control that is possible when designing security using LTMs is a definite strength when dealing with IW concerns as threats, vulnerabilities and targets are constantly changing. The problem of scalability is the need to deal with infrastructure at many (Global, National, Organisational etc) levels. This can be dealt with by bringing forward the concept of layering the LTMs so that each level of information infrastructure can have one-to-many LTMs that each depicts a security-based problem/solution pairing. Any number or level of information infrastructures can be included in the overall model. This way of dealing with issues allow the entire organization to deal with security as a cultural issue rather than leaving the task up to management armed with baseline methodologies, and an ever increasing work load.

The problem of cost evaluation influencing critical system security is solved, as

LTMs do not make cost evaluation a major part of the decision making process. CII-based cost evaluation is virtually impossible, so factoring it in but at a lower level is a way of making sure security is built well over the breadth and depth of the system. Focusing on one seemingly major, but, actually minor area to secure can often be a downfall of organisations (Cramer 1997). The only minor difficulty is the need to classify which information infrastructure level contains particular entities, problems etc. A proposed solution to this problem is to also include scope in the modelling methodology to handle infrastructure interfaces. This would be where security issues regarding physical and/or logical links between two infrastructure levels would be discussed.

The proposal of the idea of a new LLTM-based security risk analysis model comes about as a result of the lack of suitability of the aforementioned security risk analysis methodologies to Information Warfare and CII protection (Busuttil and Warren 2002). The lack of suitability of SRA methodologies comes about due to insufficiencies in the current standards and guidelines that current infrastructure security professionals are required to work within. This next generation will involve the application of logical transformation methods across the layers of information infrastructure discussed in table 1.

3. CRITICAL INFORMATION INFRASTRUCTURE PROTECTION - RISK ANALYSIS METHODOLOGY

When building an information security system using logical transformation models there are a number of steps that need to be followed. Firstly, a system implementation participation group representing a large cross-section of the involved system users should undertake the approach as this will assist in the exposition of infrastructure definitions, vulnerabilities and countermeasures. For each defined piece of the information infrastructure the following information needs to be stored:

- Infrastructure definitions;
- An Infrastructure vulnerability assessment on each infrastructure level.

Once a vulnerability assessment has been completed the group can then attempt to map the vulnerabilities to areas of infrastructure and organisational responsibility so as to get an overall understanding of the problems that face the organisation undertaking this risk analysis approach. The following formal stages are required for completing this new method of security risk analysis:

1. Form system implementation participation group;
2. Define Infrastructure;
3. Complete vulnerability assessment on each infrastructure level;
4. Derive countermeasures based on findings from steps 2 and 3.

Stage 1 should be completed once at the beginning of the lifecycle of the risk analysis process. Stage 2 should be completed once for each piece of infrastructure that is introduced to the overall system. Stages 3 and 4 should be completed once at the beginning of the analysis to cover all the parts that exist at this time within the infrastructure system and should be updated regularly for both new and previously

integrated infrastructure entities. A step-by-step description of each of the aforementioned stages follows.

3.1 INTRODUCTION TO STAGE 1 OF CIIP-RAM

The first stage in CIIP-RAM (Critical Information Infrastructure Protection – Risk Analysis Methodology) was originally to construct a committee with a wide cross-section of understanding regarding the current computing environment within the organisation in which the risk analysis is being undertaken. This committee was designed to encompass people from all levels of the organisation e.g. management to clerks, and also different areas of expertise e.g. computing to accounting. The reason for this diversity to be inherent within the panel undertaking the analysis is that the organisation are looking for all information infrastructure security risks and the wider the net is cast the more likely each ensuing stage will be completed to an efficient level.

The concept of bringing people's concerns to the discussion table or at least voicing opinions is believed to be an important step in constructing systems that are efficient (Mumford and Henshall 1979). However, the major goals of forming a committee are often not met if a leader champions the group with strong views toward an issue or with a preconceived and/or stubborn approach to the process (Davey 2002). In view of this situation, a more effective approach to the first stage of the methodology is to accept representative views in electronic form and allow computing technology and a system operator to take the form of a trusted third party which offers pre-programmed cataloguing and indexing of the problems and formulates them in a way so as to allow easy understanding of where the problem lies, who is affected and also when and how the problem occurs or has occurred in the past. This approach offers two major advantages over the original committee-based approach. Firstly it allows issues to be raised in an unfettered manner by the system implementation participation group and secondly, the results are stored in an easy to read and recall environment which can be access controlled. This method of system development has been characterised by the Joint Application Development (JAD) methodology originally employed in the early 1970's by IBM as a way of designing systems which fit requirements of all the users. JAD required a number of participants from all areas within the project scope as well as outsiders to discuss and document the system requirements whilst also communicating with those who would ultimately use, implement and maintain the system (Hoffer et al 2002). It was originally designed to cater to the creation of computing and information systems. The creation and implementation of a security policy is similar as there is a final goal and an ongoing, sign-posted, evolutionary process to achieve this goal.

3.2 CIIP-RAM Stage 1 – Form system implementation participation group

Stage 1 of CIIP-RAM is described in detail within sections 3.2.1 – 3.2.3.

3.2.1 CIIP-RAM Stage 1.1 - Assemble Group of Stakeholders

The first step toward the application of the CIIP-RAM methodology is the assembly of a system implementation participation group. The main focus of this group is to collect and present, without prejudice or bias, the concerns of the stakeholders, users, developers etc. of the new security culture. Using either a manual or computer-based system, depicted in figure 1, as a tool for information collection this group should see the first implementation cycle through whilst also ensuring that new system entities be they human or non-human are kept informed, updated, secured and involved with new and changing policy.

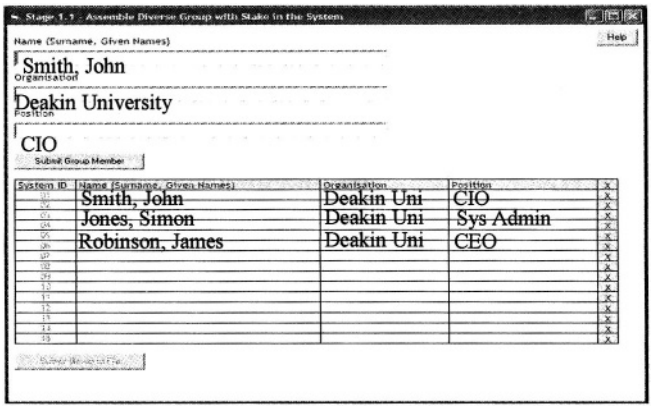

Figure 1 : Screenshot depicting CIIP-RAM System Step 1.1 (Section 3.2.1)

3.2.2 CIIP-RAM Stage 1.2 - Instruct Group as to the Goals of the Exercise

The instruction of the group as to the goals of this new exercise is a crucial step in the creation and sustainability of new policy and culture. It is important that the group members can understand the need for change in security policy and culture through training with regards to goals of this exercise. It is also important that group members are able to communicate to other members of the organisation in a concise manner what changes will be put in place and the reason for these changes. The ability to put forward new and unforeseen issues and problems is also a key task for system implementation participation group members. The overall goal of the exercise is to eradicate information infrastructure vulnerability whilst taking into consideration stakeholders within the system. This should not only be the goal of the exercise but also the goal of each member of the group and in turn the organisation.

3.2.3 CIIP-RAM Stage 1.3 - Instruct Group on the steps involved

The CIIP-RAM system is a methodology which is designed to be followed stage-by-stage. It is important that the group knows what each of the steps are, what they must do singularly and as a team to fulfil each step. Most critically, the maintenance of the culture change that the use of this methodology will likely invoke must be taken into consideration at this stage. Each group member should be given information on the process as well as step-by-step instructions on how to manage and execute the methodology. At the point where all group members have read and understood what the process will entail, group consensus should be reached with regard to any perceived problems or ambiguities.

3.3 INTRODUCTION TO STAGE 2 OF CIIP-RAM

This stage requires the committee to classify what sort of CII it is dependent on. An organisation makes use of an organisational CII that administers personal IIs whilst being reliant on a NII. At this stage the system boundaries (Vidalis and Blyth 2002) should be mapped so as to understand where different LTM's are required for different layers of II. The total OII should be broken down into sections that can be defined, classified and analysed separately. This definition of infrastructure entities may include a mapping to the infrastructure, including its interfaces to other infrastructure within and outside of the organisation as well as the current security measures currently in place. Previous security incidents (if any) and the relevant countermeasures taken (if any) would also assist in the further steps in the model. It is important to remember that the focus of stage 2 is to derive the organisational CII and despite the use of PIIs, NIIs and GIIs to derive the scope of the organisational CII these other IIs are not really important to the undertaking of the CIIP-RAM.

3.4 CIIP-RAM Stage 2 – Define Critical Information Infrastructure

Stage 2 of CIIP-RAM is described in detail within sections 3.4.1 – 3.4.5.

3.4.1 CIIP-RAM Stage 2.1 - Define the Information Infrastructure

The definition of the information infrastructure should be completed using two basic methods. Firstly, a diagrammatic depiction of the Information infrastructure should be derived, perhaps using UML or some other information-rich graphical representation. The diagram should show, to the greatest possible detail, systems, entities, links etc. The diagram should deal with multiple infrastructure levels from high-level (offices in London and New York) to low-level (computers linked in room x of building y via null modem cable). The depiction of these scenes helps in the understanding of networked infrastructure.

It is also an extremely important part of this step to textually show relationships between network infrastructures. Once again this should focus across the width and breadth of the organisation and should be completed with as much detail as possible.

The completion of both the diagram and the written form will allow for the system implementation participation group to have a clear and detailed view of their organisational world. The group should review the two depictions and clear up ambiguities and imperfections before moving on to the next step.

3.4.2 CIIP-RAM Stage 2.2 - Define the System Boundaries

In defining the system boundaries the group must work toward understanding which infrastructural entities they do or do not own and control. Demarcation of the boundaries helps the group understand the scope of the information infrastructure they are working within. The group should then review the information infrastructure definition they have derived so as to exclude all infrastructure entities outside these new boundaries.

3.4.3 CIIP-RAM Stage 2.3 - Define Manageable CII Sub-Systems

At this stage the group will have a reasonable understanding of the infrastructural entities they must protect as well as a pre-existing knowledge of the organisational processes that are undertaken by them and their colleagues. The next task is to break down the newly defined information infrastructure into more manageable and critical subsystems. The splitting of these systems can be done in numerous ways but, the simplest ways are grouping by physical location (systems in London and New York become sub-systems) or by logical connection (payment systems and database systems become sub-systems) or a mixture of both. These newly derived sub-systems should be of manageable size. If this has not been reached then further division of systems shall be done by the group until this requirement is met. This information should be entered into the CIIP-RAM system step 2.3 as depicted in Figure 2.

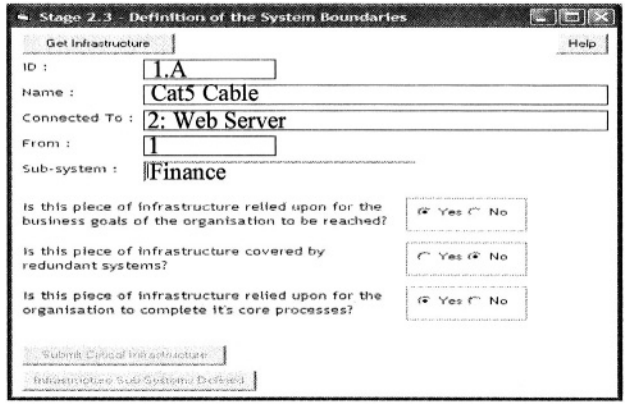

Figure 2: Screenshot depicting CIIP-RAM System Step 2.3

3.4.4 CIIP-RAM Stage 2.4 - Breakdown Sub-Systems into Classifiable Infrastructure Entities

Considering now the derived information infrastructure sub-systems, it is an important next process to further break down these systems into the entities that make up the system. In the case of this review an entity is defined as any infrastructural hardware device, information store, connection mechanism or person. These entities should be mapped out both textually (Figure 3) and diagrammatically as was completed in the previous step and using similar methods and syntax to show relationships.

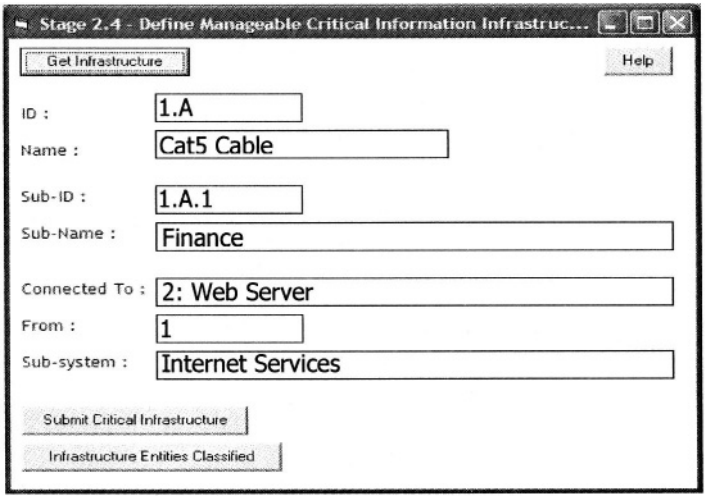

Figure 3: Screenshot depicting CIIP-RAM System Step 2.4

3.4.5 CIIP-RAM Stage 2.5 - Enter Information about Each Entity

The entering of information captured within this phase is an important step in the infrastructure definition process. The major goal of this exercise is to capture the information that is currently known about the entity in question. The required information and a method for capturing that information is shown in Table 1.

Table 1. An example of a classification table

Classification	Explanation
Sub-System	Payment Systems Support
Entity	Workstation 6
Connections	Payment Systems Support LAN via CAT5 cabling
Security in Place	Dumb terminal status, password access
Past Security Problems	(July 1997) Subversion of password controls
Solutions Applied	(July 1997) Changed password

It is noticeable that the sub-system, Entity and connection fields have different colours applied to them. The blue depicts a subsystem name, red depicts an entity name and green depicts a connection mechanism. It is crucial that differences between these three are noted and marked in some way. Doing this makes the understanding of the model easier to derive information from at a later date. At the completion of this step the system implementation participation group should have a compiled list of entities and the information known about each. It is important that this information is conserved for use in further steps and also as a reference.

3.5 INTRODUCTION TO STAGE 3 OF CIIP-RAM

The third stage requires the completion of a vulnerability assessment which should include a thorough rundown of likely vulnerabilities within the organisation as a whole and also any known vulnerabilities within its connection scope to particular entities within the OII. A method of vulnerability assessment within the scope of electronic payment systems (EPS) named 'Threat Assessment Model for EPS' (TAME) (O'Mahony et al. 1997) shows a loosely coupled decision loop that allows for on-the-fly adjustment to system threats and inputs and outputs (Vidalis and Blyth 2002). The steps involved in this system are useful; however it is important to know where an organisation is in the security process. The TAME system also focuses greatly on assessing threat which takes impetus away from finding vulnerabilities within the organisation. Concentration on threat as opposed to vulnerability can cause security weaknesses to go unnoticed as there may be a threat that can never be prepared for. If the organisation attempts to keep vulnerabilities to a minimum then it is not overly important to know the nature of the threat agent (Malone 2002).

The new methodology takes into account the following contiguous stages:

- Assessment Scope;
- Scenario Construction and Modelling;
- Vulnerability Analysis;
- Evaluation.

The stages consist of a number of steps which should be completed in turn so as to be easier to follow and keep track of. The concepts covered in the new methodology are similar to those discussed in the TAME system.

3.6 CIIP-RAM Stage 3 – Complete Vulnerability Assessment on Infrastructure Levels

CIIP-RAM's third stage is described in more detail in sections 3.6.1 – 3.6.4.2.

3.6.1 CIIP-RAM Stage 3.1 - Prepare an Assessment Scope

The preparation of an assessment scope is a two step process which consists of the completion of a Business Analysis and a Stakeholder Identification.

3.6.1.1 CIIP-RAM Stage 3.1.1 - Complete a Business Analysis

A basic business analysis in accordance with (Nosworthy 2000) involves the process of business goal and business process identification. In addition to undertaking the basic business analysis the inclusion of an environmental analysis should also take place as a means of examining the environment within which the organisation exists.

3.6.1.1.1 CIIP-RAM Stage 3.1.1.1 - Identification of Business Goals

The identification of business goals is of key importance in any risk analysis application as it allows the system implementation participation group to bring major issues requiring review to the forefront of the risk analysis (Forte 2000). The identification of the business goals can be determined by stakeholders of the organisation that is the subject of the analysis.

3.6.1.1.2 CIIP-RAM Stage 3.1.1.2 - Identification of business processes

With the identification of an organisation's critical business processes we are able to bring to the surface more assets and vulnerabilities. A number of organisational primary and support processes could be identified (Johnson and Scholes 1999) at this time and should be updated as conditions and processes change. Depending on the size of the organisation under analysis three to eight organisational processes could be identified and should be noted. These processes can later be used as scenarios in the system modelling step. An in depth description of these processes should be produced. From these details the system implementation participation group will be in a position to identify and note more assets and vulnerabilities to add to the database.

3.6.1.1.3 CIIP-RAM Stage 3.1.1.3 - Environmental Analysis

The completion of an environmental analysis is based on Porter's five forces approach of examining the business environment at the strategic level (Johnson and Scholes 1999). Three environments are identified as targets for this analysis, technical environment; business environment and; physical environment.

The environmental analysis is a reasonably basic step which consists of breaking down the three environments mentioned via discussion and getting a feel for the organisations position with regards to each of the five forces in each of the organisational environments and noting down findings. This step will further help in the fleshing out of the issues affecting the organisation.

3.6.1.2 CIIP-RAM Stage 3.1.2 - Identify Stakeholders

Each infrastructure entity will have a set of stakeholders that can be questioned in an effort to define its function, nature and scope. There are three distinct classes of stakeholder within systems according to Sutcliffe (1988), The management

stakeholders; The user stakeholders and the development stakeholders.

How ever customised stakeholder classifications can be used in each case. This would be dependent on the type of business the organisation is involved in. A list of each stakeholder should be constructed and each entry on the list is required to give input on assets and vulnerabilities that they can identify. The invocation of infrastructure protection should be looked at as an entire-organisation initiative rather than a one person job for the computer security guru. In the current environment it is important that all stakeholders in an organisation form a formidable information infrastructure protection team (Wood 1997).

3.6.2 CIIP-RAM Stage 3.2 - Scenario Construction and Modelling

Scenario construction and modeling is made up of the following steps; (1) Scenario Generation; (2) System Modeling; (3) Asset Identification.

3.6.2.1 CIIP-RAM Stage 3.2.1 - Scenario Generation

In this step the parties involved in the system implementation participation group are required to come up with a scenario involving the organisation and its use of the particular infrastructure entity under discussion. The parties that should be involved predominately at this step are the management of the company along with the stakeholders in cooperation with organisational security staff. The scenario should describe a real world application of the organisation. Risk assessment should be conducted with this, and similar, scenarios in mind. This step goes a long way toward helping all members of the system implementation participation group understand the nature of vulnerabilities across the organisation. Getting all members involved in the discussion of an area that is not necessarily within their jurisdiction can assist in the uncovering of widespread, endemic or multi-organisational vulnerabilities.

Although probably not necessary at this stage, more assets and vulnerabilities are likely to be identified. The more a particular scenario is refined and understood the more likely the group is to continue to uncover hidden aspects and vulnerabilities of a system. In addition, because each stakeholder is constructing a scenario, all likely to be from differing standpoints, it would be difficult for the system implementation participation group to not uncover the majority of the issues regarding the system under review. These scenarios are then filtered for similarities to provide a less cluttered view of the reviewed system.

3.6.2.2 CIIP-RAM Stage 3.2.2 - System Modelling

This step involves the system as a whole being modeled. All its aspects, procedures resources and transactions will be analysed in great detail. The system implementation participation group should try and take a high level view of the system. The more complete and detailed the model is at the completion of this step, the more successful the further stages are likely to be. Once again, further issues, assets and vulnerabilities are expected to be identified. If these new found attributes

fall within the scope of the assessment they should then be included in the appropriate list.

The method that the user will employ to model the CII of the organisation is to enter the names of each of the infrastructure components into the data collection mechanism and also mention connections that each infrastructure entity has with other entities in the system. With the group working toward this system comprehension it is unlikely that systems and entities will be overlooked.

3.6.2.3 CIIP-RAM Stage 3.2.3 - Asset Identification

The entries of the asset list, relevant to the scope under which we see the critical information infrastructure and its components, as well as the system procedures involved in the system transactions that we want to examine, should be included and denoted. The user should identify all examinable assets at this stage. Further assets will be identified during other steps.

The assets uncovered at all stages up to this point should then be entered under the following categories in the asset table (Nosworthy 2000), Software, Hardware, Data, Administrative, Communications, Human Resources and Physical. It is not necessary for the table to contain all the asset categories. The selection and inclusion of categories is dependent on the scope of the CII.

3.6.3 CIIP-RAM Stage 3.3 - Vulnerability Analysis

The 'CIIP-RAM Stage 3.3 - Vulnerability Analysis' stage requires users to complete stages 3.3.1-2 for each vulnerability.

3.6.3.1 CIIP-RAM Stage 3.3.1 - Vulnerability Type Identification & Selection

Vulnerability can be noted as a weakness in the security system that might be exploited to cause harm or loss (Pfleeger 1997). So with that we can safely say that a CII vulnerability is a weakness in a CII security system that might be exploited to cause harm or loss. This methodology will focus on the CII vulnerabilities. The vulnerability list structure put forward by Neumann (1995) is the method of reporting that will be used (Table 2).

Table 2. An example excerpt from an entity-vulnerability list

Entity	Vulnerability
1.4 - Web Server	Software not up to date
	Virus signature file out of date

With systems such as CIIs with so many aspects, variables and hierarchical levels it is important that we complete the step of vulnerability selection so as to make the methodology easier to follow and more usable. The completion of a vulnerability selection can help simplify and tailor the system so that it is more manageable. The user can select the vulnerabilities of one type e.g. web server vulnerabilities and tailor the system to deal with the focused problem.

However, this step could also be avoided entirely so as to give an extremely detailed look at the system from all points of view. The final vulnerability list needs to be combined with the entity list in order to get a matrix which depicts all the vulnerabilities for each entity. By doing this the user sets-up a link between entities, vulnerabilities and countermeasures. Within the computer-based CIIP-RAM management tool being developed currently, the procedure of linking the entities, vulnerabilities and countermeasures (Figure 4) will be automated to deal with complexity on-the-fly

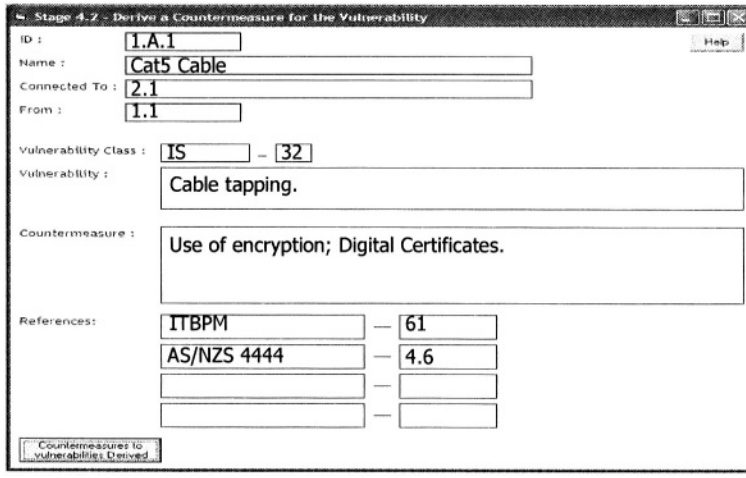

Figure 4: Screenshot depicting automated data entry from the CIIP-RAM System

3.6.3.2 CIIP-RAM Stage 3.3.2 - Vulnerability Complexity Analysis

It is important that for each entity/vulnerability pair, a certain amount of analysis be done on how many levels of security a threat agent would need to go through to exploit a vulnerability. If multiple vulnerabilities need to be exploited before a particular database server is compromised then these vulnerabilities need to be broken down into their composite vulnerabilities. These 'new' vulnerabilities should then be fed back into the matrix for further assessment.

3.6.4 CIIP-RAM Stage 3.4 - Evaluation

The 'CIIP-RAM Stage 3.4 - Evaluation' stage requires users to complete stages 3.4.1-2 for each vulnerability.

3.6.4.1 CIIP-RAM Stage 3.4.1 - Stakeholder Evaluation

In this step the stakeholders of the Critical Information Infrastructure under discussion should review the outputs of all the other stages. As with any computing related system it is important to the success of the project for the developers to stay in close contact with the client (Pressman 2001). In all cases the developers will be the system implementation participation group and the clients are representatives of the stakeholders of the CII under discussion.

Entities and vulnerabilities are expected to be introduced, or excluded, not from

the model, but from further investigation from the current iteration of the system. Once an entity or vulnerability has been introduced to the system it is important that it not be taken out. Entities and vulnerabilities may, at the first iteration, seem trivial, however due to the dynamism of computing, they may come into play during a later iteration.

3.6.4.2 CIIP-RAM Stage 3.4.2 - Vulnerability Statement Generation

After the completion of the previous step in the methodology, the output will be a number of vulnerabilities related to an entity of a critical Information Infrastructure. In this step we will produce a final table which categorises entities, vulnerabilities and a list of associated countermeasure option/recommendations. As each infrastructure entity is denoted as critical it is important that each vulnerability is dealt with as though its exploitation could be fatal to the system infrastructure.

3.7 INTRODUCTION TO STAGE 4 OF CIIP-RAM

The final stage in this security risk analysis is to derive countermeasures for the vulnerabilities that were identified in the vulnerability assessment. These countermeasures should attempt to solve the security problem being faced whilst also attempting to maintain a reasonable degree of subjective cost benefit. The derivation of countermeasures can be done in many ways including the concurrent application of bug fixes, patching, staff training new software solutions etc.

The formal presentation of these countermeasures should be delivered as shown in table 3 in the instance of each vulnerability:

Table 3. Basic example of a countermeasures table

Vulnerability	Derived Countermeasures
Apache Server security hole	Install and correctly configure firewall to assist halting of DOS attacks

3.8 CIIP-RAM Stage 4 – Derive, Apply and Analyse Countermeasures

Based on the recommendations put forward as an output from the previous stage the system implementation participation group should at this stage research the countermeasure solution space. The group should provide a selection of a finite list of possible countermeasures and should work toward an efficient solution to the problem.

From the short list of solutions provided as output from the previous task, a counter measure should be derived and formally described so as to provide a non-ambiguous process of countermeasure application.

Users then apply the countermeasure that is the output from the previous task in a correct, thorough and compatible manner. It is important that the informing and training of staff that are required to deal with the newly implemented countermeasure be completed in an efficient and thorough manner also.

After an agreed upon period of time after the application of the countermeasure it is extremely important to complete an analysis of the applied countermeasure. This analysis should include:

- Testing of the functionality of the system post-implementation;
- Mock exploitation of the originally perceived vulnerability in the post-countermeasure environment;
- User training comprehension of the new environment.

These three analyses sequences respectively should ensure that the system:

- Still does the job it designed to do in light of the newly applied countermeasures;
- Is more robust in a security sense post-implementation and;
- Is fully understood by the users of the system.

4. FUTURE RESEARCH

The major direction of this research at the current point is to derive a web-enabled version of CIIP-RAM which can be put into place to allow the security risk analysis process to be undertaken in an online environment. This product would allow for a more easily workable and hence more efficient final methodology.

5. CONCLUSIONS

CIIP-RAM is a move toward dealing with scalability issues that have meant that RA was not immediately adaptable to information warfare and other information infrastructure protection requirements. This methodology would prove to be helpful to organisations with mid-level infrastructure such as an organisational information infrastructure if undertaken in solitude however the true benefits of this methodology would be seen if it was put into practice by higher level infrastructure stakeholders. This uptake by higher-level infrastructure would lead to higher dependability and reliability being built into infrastructure system from the outset. Information warfare needs a unique security methodology that is useful at dealing with all the previous concerns that Computer Security and Information Security dealt with along with the ability to be adaptable and scalable also. When researching existing methodologies, logical transformation models proved to be a suitable method for coping with adaptability issues. The scalability issues are dealt with through the application of multiple layers of LTMs. Cost evaluation has been found to be an outdated function when analysing IW risks, LTMs have the added feature of being solution-oriented and independent of any cost evaluation procedures.

5. REFERENCES

Baskerville, R. (1993). Information Systems Security Design Methods: Implications for Information Systems Development. *ACM Computing Surveys* 25(4): 375-414.

Beer, S. (1984). *The Viable System Model: its provenance, development, methodology and pathology.,* Eds. Espejo, R. and Harnden, R., John Wiley, Chichester, UK.

Busuttil, T. B. and Warren, M. J., (2001a). An Information Warfare Protection Method. *Conference Proceedings of EUROMEDIA 2001,* SCS, Valencia, Spain.

Busuttil, T. B. and Warren, M. J. (2001b). Intelligent Agents and Their Information Warfare Implications. *Conference Proceedings of the 2nd Australian Information Warfare & Security Conference 2001,* We-Bcentre, Perth, Australia.

Busuttil, T. B. and Warren, M. J. (2002). A Conceptual Approach to Information Warfare Security Risk Analysis, *Conference Proceedings of the 2nd European Conference on Information Warfare,* London, UK.

Cramer, M. L. (1997). Measuring the Value of Information. *NCSA InfoWarCon 97,* USA.

Cramer, M. L. (1998). Information Warfare: A Consequence of the Information Revolution. *The Information Revolution: Current and Future Consequences.* A. L. Porter and W. H. Read, Ablex Publishing Corp, USA.

Davey, J. (2002). Comment made at *'Information Warfare'* Workshop, 3rd Australian Information Warfare & Security Conference 2002, We-Bcentre, Perth, Australia.

Forte. (2000). "Information Security Assessment: Procedures and Methodology." *Computer Fraud & Security* 2000(8): 9-12.

Hoffer, J. A., George J. F., Valacich, J. S., (2002), *Modern Systems Analysis and Design,* Prentice Hall, New Jersey, USA.

Hutchinson, W. and Warren, M. J., (2001). *Information Warfare - Corporate Attack and Defence in a Digital World.* Butterworth-Heinemann, Oxford, UK.

Johnson, L. S., (1997). Toward a Functional Model of Information Warfare. Studies in Intelligence 1(1).

Johnson and Scholes (1999). *Exploring corporate strategy,* Prentice Hall Europe.

Libicki, M., (2000). *The Future of Information Security,* Institute for National Strategic Studies: 10, USA.

Malone, J., (2002). Comment made at *'Information Warfare'* Workshop, 3rd Australian Information Warfare & Security Conference 2002, We-Bcentre, Perth, Australia.

Molander, R. C., Riddile, A. S. and Wilson, P. A., (1996). *Strategic Information Warfare: A New Face of War.* RAND Corporation, Washington, USA.

Mumford, E., Henshall, D., (1979), *A Participative Approach to Computer Systems Design,* Associated Business Press, London, UK.

NCS., (1996). *Risk Assessment: A Nation's Information at Risk.* Arlington, Virginia, National Communications System, USA.

Neumann, (1995). Computer Related risks, Addison-Wesley.

NIPC., (1996). *Critical Infrastructures,* National Infrastructure Protection Center - US Government. USA.

Nosworthy (2000). "A Practical Risk Analysis Approach: managing BCM risk." *Computers & Security,* 19(7): 596-614.

O'Mahony, D., Peirce, M. and Tewari, H. (1997), *Electronic Payment Systems,* Artech House Inc.

Pfleeger (1997). *Security in Computing,* Prentice Hall Int.

Pressman (2001). *Software engineering: A practitioner's approach,* McGraw-Hill.

Sutcliffe (1988). *Human-Computer Interface Design,* Macmillan Education.

Vidalis, S. and Blyth, A. (2002). Understanding and Developing a Threat assessment Model, *Conference Proceedings of the 2nd European Conference on Information Warfare, London, UK.*

Wood (1997). "Policies alone do not constitute a sufficient awareness effort." *Computer Fraud & Security* 1997(12): 14-19.