Global Information Assurance Certification Paper

Hard Earned Lessons In Implementing Computer Security Incident Response

Name: Jason Chee
Date: 3rd July 2003
Version: GIAC Security Essentials Certification (GSEC) Practical Assignment 1.4b

Abstract

The intention of this paper is not to serve as a guidebook for creating a computer security incident response process. My intent is to share with the security community the issues that I experienced when implementing a computer security incident response process for my organisation. It is hoped that others will have a snapshot of the way we implemented our process and the consequences of the decisions made along the way. I will end this paper with some key lessons learnt to hopefully assist other to prepare when the time comes to implement their own security incident response process.

As a background, our organisation employs over 20000 staff and is publicly listed on the Australian Stock Exchange. The project team consisted of a project manager and two subject matter experts, which I am one of. My role is to primarily document the process and procedures of computer security incident response. At the time selecting this topic to write, I had hoped that our "computer security incident response" project would be at a stage where a test run had been conducted to see the results. However due to unfortunate circumstances implementation has taken a little longer than expected. As I hope to explain, promoting a computer security incident response process to an organisation this size is no small feat.

Before Snapshot

In the past

Most organisations that rely on computers to remain viable in business have some sort of process for maintaining the uptime of their systems. Common procedures such as incident management, crisis management, contingency plans exist to ensure that systems are available most of the time. Furthermore, it is common practice for the performance of technology support teams to be measured by the number of hours that systems have been offline during a given period. Hence it is not difficult to see why security is often neglected during an incident management process.

Similarly our organisation has a sound process to ensure that availability of its systems is maintained at all times. The process and procedures to manage incidents is one that has existed for many years. Every new employee that has a role in supporting the company's systems is trained through this process. The process is well documented, simple to follow, has the customer's best interest in mind and if adhered to is fully capable of guiding technical support teams to fulfil it's goal. A goal to restore the availability of systems with the least (immediate) impact to customers.

So where is the issue?

The existing process and procedures of resolving computer problems does not distinguish between security and non-security incidents and both are treated the same. This may have been adequate in the past but today's environment suggests that security incidents need to be treated uniquely as they have extra requirements compared to everyday "problems". For example there may be a need to: retain evidence, prosecute intruders, isolate systems that could be used to infect subsequent systems or relay attacks. In some cases, following the old notion of restoring an impacted system as quickly as possible may not be the smartest move. Moreover security incidents are becoming more complex, signifying the need for computer security experts to govern investigation and recovery efforts.

Risks if we didn't change

There is undoubted evidence that the number of computer security incidents have increased over the last 10 years. As highlighted by figure 1 below, the rate of increase is growing at a very rapid rate. The number of incidents reported to CERT/CC I the last 10 years have increased by more than 20 times!

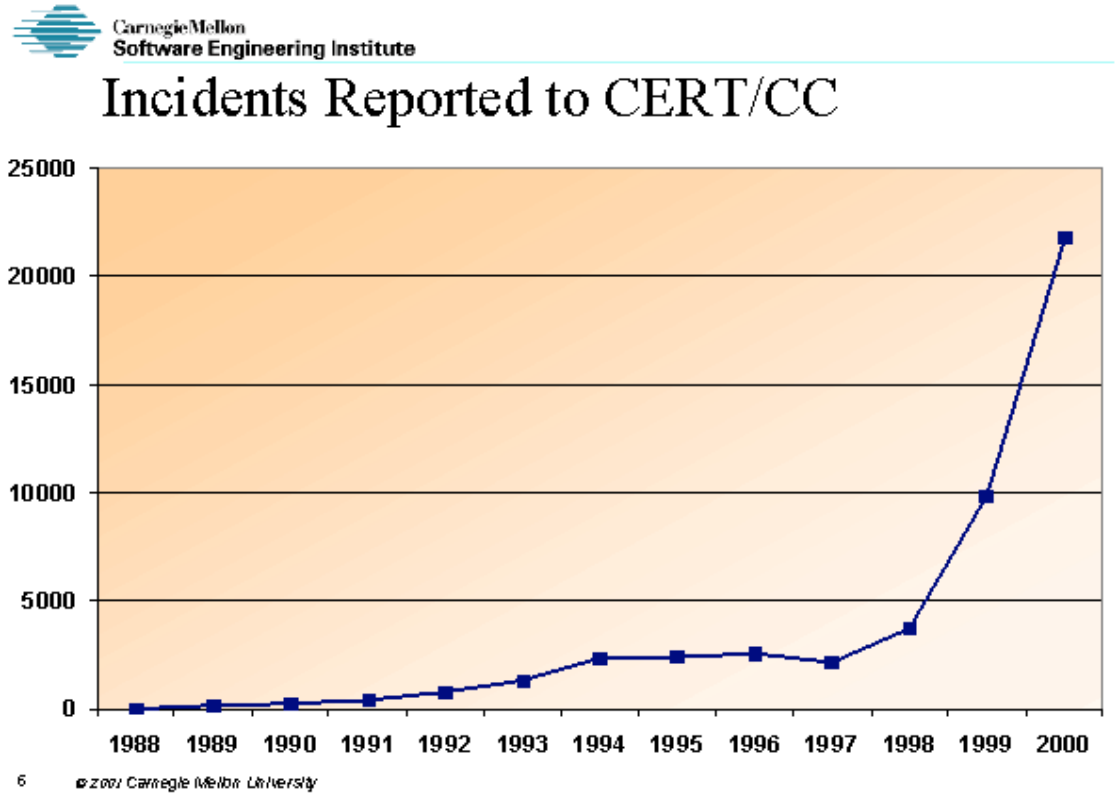


Figure 1[1]

As technology grows, both software and hardware become more sophisticated and as these grow in complexity so do the methods of attack. Code red and Slammer worm is just a couple of classic examples. Both of these are still in the wild, and if un-patched systems are connected on the Internet today, there is a high chance that it will be infected sooner or later.

[1] http://www.cert.org/present/internet-security-trends/sld006.htm

For those that have worked in an organisation of similar size and have experienced an emergency response to a security incident (or any other incidents) with no documented process, will understand that when the pressure is on, mistakes are often made. It is also not uncommon for teams to evade their responsibilities under such circumstances.

Moreover laws and regulations are beginning to regulate the organisation's responsibility to information security. Here are two examples:

1. **National Privacy Principle 4.1**. "An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure." [2]

2. **New California Privacy Law SB 1386**. "The unprecedented disclosure requirement under SB 1386, signed recently by Governor Gray Davis, is triggered upon any unauthorized access to personal data such as customer names in association with their social security, driver's license or account numbers. When a perpetrator such as a hacker or rogue insider gains unauthorized access to that data, the company must notify the affected California customers in "the most expedient time possible and without a reasonable delay."[3]

So it is quite evident that without a properly documented process to ensure the right people respond to such incidents, an organisation runs the risks of not knowing "who does what, when, how and why". Such uncertainty can lead to:

- Information leak, loss of confidentiality
- Compromise of customer's data
- Reputation loss
- Financial loss
- Loss of market competitiveness
- Loss in perceived value of the share price
- Impact more adverse to the organisation's systems than necessary

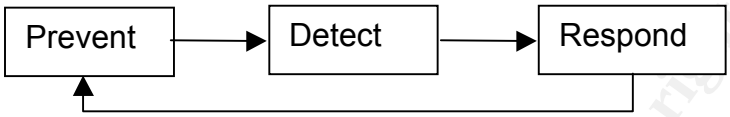
[2] http://www.privacy.gov.au/publications/npps01.html#d

[3] Zintel, Matthew

During Snapshot

Understanding the problem

Basic information security management can be summarised into the following three staged cycle.



In general, policy and compliance work to prevent security incidents. Should this fail there are measures in place such as intrusion detection systems and antivirus software that will detect an incident. Should that fail, a response process will be invoked. The information gathered from a response should then provide feedback back to policy and compliance. Unfortunately, most organisations focus heavily on the first two stages (prevention and detection), and often neglect response. The idea is that if you can sufficiently prevent an incident, there will be fewer incidents to detect and eventually we won't need to worry about response. Right? Wrong.

As mentioned previously, technology is rapidly changing. New vulnerabilities are discovered everyday. Threats are increasing. As the SANS Security Essentials courseware highlights about incidents, "its not a matter of if but when".[4]

"Experience shows that most organizations don't think about how to respond to a computer security incident until after they have experienced a significant one! This problem is common; many organizations have not assessed the business risk of having no formal incident-detection and response mechanisms in place. More often than not, organizations receive reports informing them that they are involved in an incident from some other part--rather than identifying the incident themselves!"[5].

It is only recently that our information security department was successful in driving the message to the organisation of the need to form a computer security incident response process. Although, part of this success was also due to an external security audit conducted by a reputable information technology company, which further emphasised the risk. Operational and financial support was provided and hence the "security incident response" project was born.

[4] SANS Security Essentials II: Network Security Overview p4-4
[5] West-Brown, Moira

Defining the requirements

Now that we have defined the problem, it was time to determine the exact requirements for the solution.

We began by analysing, what is it that the response process is trying to achieve? What are we actually protecting? The SANS Security Essentials courseware talks of the importance of knowing the value of your assets so that appropriate protective measures can be implemented. We then quickly identified that it would be ideal if the response process had some sort of tool to determine the value of the system to which they were responding. Here we stumbled upon a problem within a problem. The organisation currently had no means of easily identifying the value of its assets. From experience we could probably identify the top 1 or 2 most critical systems, but that would be based on knowledge based estimates. The number of computer systems that exist in our organisation is enormous. We run thousands of applications over multiple platforms. Profiling each asset to determine their value was going to require an entire project on its own! Bear in mind, knowing your asset will also assist in the prevention and detection of security incidents. So we were left with a disadvantage. Without knowing the value of our assets, it would make valued response decisions rather difficult.

This then, was a trigger for us to recognise our next issue. Given that it was not immediately possible to base response decisions on the value of assets, on what principles do we then base our key response decisions on? With over 20,000 employees structure over many departments each serving it's own objectives, defining a central decision point was going to be difficult. Ideally there should be a single point of responsibility, but in practice this was not feasible. So rather than trying to define a single point of authority we decided that there was a requirement to conduct a business impact analysis to determine the organisation's overall objectives. These objectives would then be translated into a set of, what we called, policy principles. It would then not matter who made the decisions, as long as it was made based on the policy principles, the organisation's interest would be protected.

It quickly became apparent to us that the success of an incident response process was heavily reliant on two dependencies, being valuation of assets and defining policy principles. We were faced with the predicament of whether to postpone the computer security incident response project until such time these dependencies were resolved. However, that could see the organisation without a response process for quite some time. In the interim our organisation would be susceptible to the risk of not having a response process in place. So some basic risk management came into effect. Do we strive to develop the ideal infrastructure for response and leave ourselves open for however long it took to have those in place, or do we compromise quality and cover ourselves now and build on the process as time progressed? Lets run through a simple risk

equation from the SANS Security Essential courseware. Bear in mind this equation is being applied to a process rather than a software or hardware technology:

Risk = threat x vulnerability x asset value

We recognised that the nature of our business, mainly involving money, meant that we were susceptible to many threats daily. Our Intrusion Detection System logs were able to justify this. Given that we do not currently have a defined process for dealing with security incidents, our vulnerability was quite high. Furthermore, our organisation is one of the top 100 companies on the Australian Stock Exchange so we could confidently assume that our asset values were also high.

Risk = threat (high) x vulnerability (high) x asset value (high)

The answer was clear. The risk was far too great and we needed a security incident response solution now!

"Best Practice"

Our department had a vision of being "best practice" in information security. We were striving to be recognised in the industry as the "best of breed" in information security. So the next requirement was to ensure that our project complied with our department's long-term vision. What impact did this have? The notion of "best practice" was a key driver to some of the decisions we made.

We first had to identify what "best practice" actually meant. This is a term that continues to raise debates. "Best practice" according to who? Best practice in the industry? The country? The world? After much deliberation we concluded that "best practice" was very subjective, and in doing so, came up with two criteria that would, at least, give us a level of confidence that we were heading towards "best practice". These criteria was accepted and sanctioned by the rest of our department. They were to:

1. Use existing internationally recognised standards adopted by the industry has having the "best practice" in information security
    a. SANS Incident Handling
    b. ISO 17799
    c. CERT Coordination Centre

2. Seek assistance from an internationally recognised consultant that had:
    a. Expertise and experience in computer security incident response implementation for similar industries.
    b. Adopted one or more of the standards listed above.

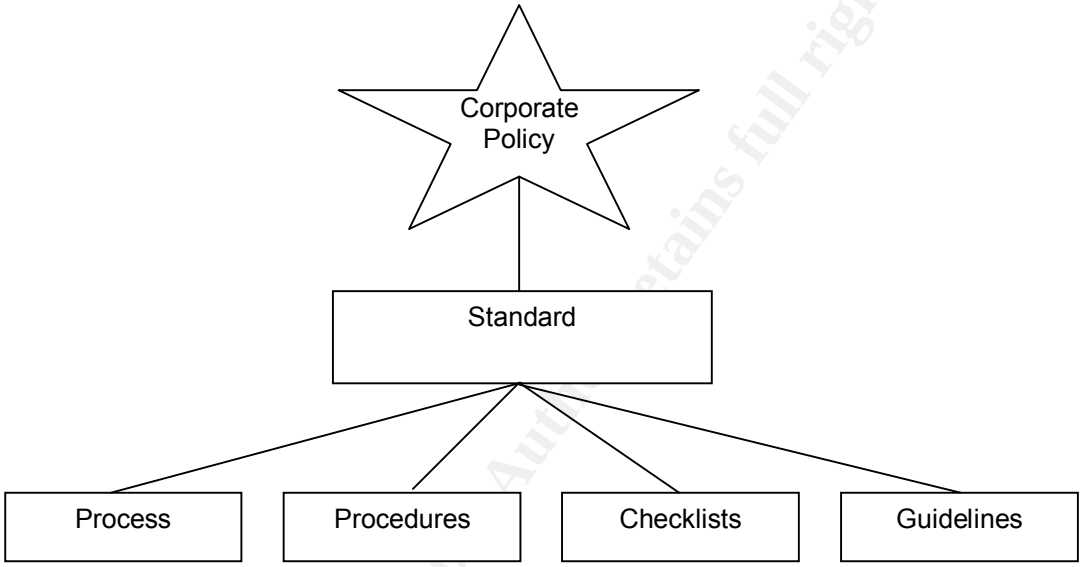
We were conscious of the fact that process and procedures is heavily dependant on the individual organisation's culture. The chances of obtaining a "best practice" response procedure from a standard or another organisation that would fit into our environment would be very slim.

"In the search for a quick fix to establishing guidelines under which a new team will operate, many people go in search of existing CSIRT guidelines with the hope that they can simply be adopted for use in their environment. However, they soon realize that no single set of service definitions, policies, and procedures could be appropriate for any two CSIRT. Moreover, teams with rigid guidelines in place find themselves struggling to adapt to the dynamic world of computer security incidents and attacks." [6]

[6] The Handbook For CSIRT p.9

Computer security incident response process development

Now that we had identified our requirements, the next stage was to develop the process. Firstly, we had to identify how to best document the process to help us meet our objectives. Below is a model of the documentation structure we adopted from Charles Cresson Wood's Security Policies Made Easy. This was the accepted framework for all security process and procedures in our organisation:

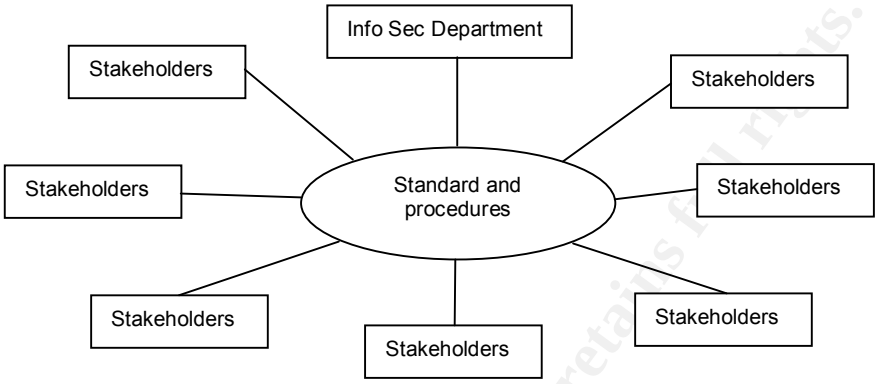


The corporate policy consisted of high-level statements mandating and giving authority to the computer security incident response standard. The standard is an operating principle consisting of a set of rules that must be met to ensure there is a consistent compliance to policy. The process, procedures, checklists, and guidelines are low-level work instructions of the response process.

The next stage of the development was to decide how to put the information into our documentation framework. This proved to be a very important decision point as it impacted the implementation stage.

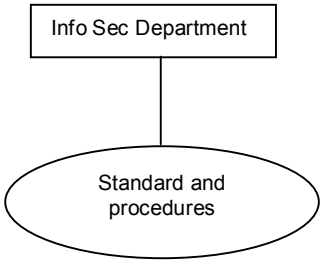
We identified 3 options:

Option 1:



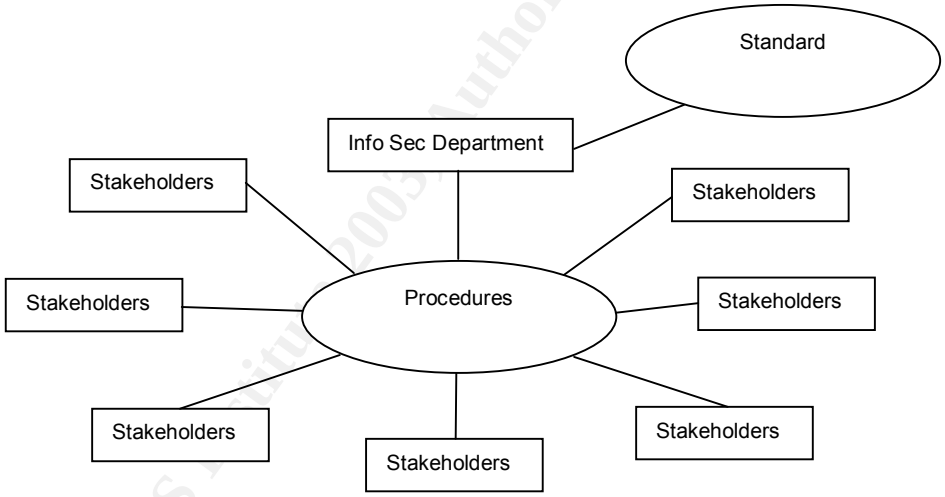
Develop all documentation with all stakeholders. This will ensure all stakeholders have an active input into the process. In theory this would be the preferred option as it ensures the buy-in of all stakeholders. However, given the number of stakeholders and the size of our organisation and the time constraints placed upon the project, this was not an acceptable option. This method also ran the risk of our current organisational practices, which may not necessarily be "best practice" according to our criteria, shaping the end result.

Option 2



Development of all documentation to be performed by the Information Security department. This option ensures that the end "best practice" result will not be constrained or influenced by current internal practices. It would also ensure that the project would be delivered in a timely manner, as only one "approver" was required. The downside is that buy-in process will be difficult, as stakeholders have had no prior opportunity for input.

Option 3



Have the standard documented by the information security department, and let the relevant stakeholders own the procedures. This still inherits the risk that procedures could be influenced by the organisation's current practices.

After many long discussions option 2 was taken. Project's tight timeframes and the emphasis on "best practice" was a major influence in the decision. However we did factor in the risk for implementation resistance.

Now that we have our documentation pencilled in, it was time to consider where were the people required to make the process work. Computer Security Incident Response Team (CSIRT) is almost always referred to when talking about response team for computer security incidents. Why do we need a CSIRT?

Here are some reasons from the Computer Security Journal[7]. A CSIRT will provide:

Ability to coordinate	A team leader to direct and organise individuals on a response team
Expertise	Information security incidents are becoming increasingly complex; incident handling experts are thus becoming increasingly necessary.
Efficiency	A team builds a collective knowledge that often leads to increase efficiency.
Ability to work proactively	Having a team increases the likelihood that proactive efforts will occur.
Ability to meet corporate requirements	A team is generally better suited to meeting corporate requirements.
Serving a liaison function	Having a team identity provides extra external visibility as well as credibility, both of which are more suited to the liaison function.
Ability to deal with institutional barriers	Incident response teams provide at least some degree of immunity from politics that provide barriers to incident response efforts.

Our project team explored the idea of a CSIRT and ran through some scenarios on how the team could be structured. Should we outsource to a 3rd party response team? Should we have designated members to respond to all incidents? Should it be a virtual team? We recognised that the people within our organisation are talented and capable to resolve most incidents relevant to their job role. Coupled with cost constraints, it was decided that a virtual team structure was the best CSIRT formation for our organisation, whereby there would be two or three designated CSIRT Leaders. Internal staff, based on the nature of the incident, will form the rest of the response team. This empowered all staff the opportunity to become part of the process and hopefully ease the process implementation.

[7] Schultz, Eugene p.2

After Snapshot

The selling factor

The policy, standard and procedures had been "completed". The information security executive had approved all documentation. Furthermore the consultant had endorsed the process as "best practice". Now it was time to promote and market this new process to the people required to do the job.

Just to give you an appreciation on the magnitude of the selling factor, here are just some of the main departments with direct impact:

- Security
- Risk
- Investigations
- Technology support groups (for which there are many)
- Human Resources
- Media Relations
- Legal

Not all these departments report to the same business unit head. As you can imagine, the size and structure of our organisation meant that we had to "intrude" into business units outside of our own. This was a daunting task as it put us into a zone not governed by our management. I can't stress how important leadership and support from senior executives is required in these circumstances.

As we had expected, there were some resistance encountered during the initial implementation phase. Without dwelling into the specific issues of each department, here is a summary of the major concerns raised.

"Why weren't we informed of this problem from the beginning?"

"I own the asset, what gives the CSIRT Leader authority to tell me what I should and shouldn't do?"

"Who is the leader?"

"How will the leader make decisions?"

"How is this going to directly impact us?"

"Will we be trained?"

"This process and procedure is too long and hard to understand. It will never work"

On the surface, some of these concerns seemed quite threatening to the project initially. However, further analysis revealed that the major problems were not with the actual process and procedures itself.

As expected, the decision to proceed with option 2 for documentation development was an issue in itself. Initial communication of the project was a phase that we had significantly underestimated. We operated based on the assumption that policy, with the approval of senior executives, would give sufficient authority for the response process to be implemented with little resistance. Although if push came to shove the policy ultimately had the strength to do so, we realized that this was not the best method to promote information security to the organisation. Rather, we decided to sacrifice a little delay in the project to ensure that the organisation would accept the process.

Majority of the issues raised were more misunderstanding of the context of the documents. For example the business had difficultly understanding how confidentiality, integrity and availability translated to the overall business objectives. Another example was that, it was initially suggested that during an incident, response team members should "report to the CSIRT Leader". This language was too aggressive and so a passive tone such as "supports the CSIRT Leader" was more acceptable. The reason I highlight this is not to dwell on the politics, but to exemplify the need to be sensitive to such issues in a large organisation.

Other departments found the entire response process overwhelming. The procedures consisted of numerous steps of which only a few were relevant to each individual. As such, we decided to segregate the procedures into three parts and implemented them in phases:

1. Identify and Communicate – raising the alert and calling the right people.
2. Solve – to contain, eradicate and recover.
3. Report and Track – ensuring process improvement and post incident analysis.

The concern of authority was an interesting one as the process clearly stated that the asset owner had primary authority to make key decisions so long as it was based on the accepted policy principles. We found that the majority of the people we spoke to had misconception of a CSIRT. They immediately perceive CSIRT as a team who played God. This was clearly not our intention.

Quite clearly a majority of the concerns raised were based on the fear of change. The misconceptions were an effect of fear. Fear of how this will impact individual's teams. Fear of extra workload. Fear of doing something wrong. Fear of not understanding the procedures. Fear of loosing authority during a security incident.

It became apparent to us that our mission was far from over. Whilst we had "best practice" process and procedures, these would not be effective if the organisation did not embrace the change. With this in mind, our project team is now working overtime to engage with change management to help guide impacted staff through this change process. It is envisaged that this "problem" will be addressed on an ongoing basis probably for the next 3 to 6 months and will not be solved overnight. As of today, we have opened our policy, standard and procedures for discussion, giving each stakeholder an opportunity to formalise feedback, with strict regulations against changing rules that could deviate us from "best practice". Our key message is that the organisation had to change the way they do things to meet "best practice" and not change "best practice" to meet current practices. In some respects we have reverted to option 1 of the documentation development. The good news is, as of this moment we are already making some key wins! For instance procedures for the portion to Identify and Communicate incidents have been accepted and taken to practice. This is a significant headway in comparison to where we started.

Lets revisit our risk equation and find out whether we have made any improvements:

Risk = Threat x Vulnerability x Asset Value

Our threat and asset value remain high. These were variables beyond the control of the project. Although not all the procedures have been implemented, the ability to identify and communicate incidents is a key milestone. As such it is fair to say that we have made some headway into reducing our vulnerability, and therefore our risk has been reduced moderately. A slight improvement from where we started.

Lessons Learnt

Here is a summary of the key lessons learnt from my practical experience in implementing a computer security incident response. Although each organisation is unique politically and in size and structure, I trust that these lessons will be of benefit to other CSIRT implementations in some shape or form.

1) It is a lot easier to propose an organisation process improvement if you can justify it through a independent party. Anything to increase management confidence that they are spending their budget for a good cause. In our case we used a reputable external consultant. Other options may be to approach an internal auditing team, investigations team or a risk management team to support the cause.

2) For those contemplating to implement a response process but are hindered by dependencies, bear this in mind. The risk of not having a response process far outweighs the benefits of waiting for the ideal supporting infrastructures. A security incident response is an evolving process and will be subject to continuous improvement.

3) Translate your information security objective to a language that the rest of your organisation can understand. For example, relate "confidentiality, integrity and availability" to "shareholder value, market opportunity and regulatory compliance". Be sensitive of the language used in documentation. Whilst you want to stamp down the process and procedures you do not want to threaten staff that are vital to its success.

4) Where possible make the CSIRT a virtual team. This gives everyone in the organisation a sense of involvement and should make the idea easier to accept.

5) Implementation of the entire response process can be overwhelming to individual departments of an organisation. Where possible, segment the procedures and provide only the relevant portion to each individual department. However it is important that everyone understands how these smaller portions fit together to achieve a common goal.

6) Most importantly, plan for change! Reality is that an organisation is a lot like a football league. The league is made of many teams. The league is established to achieve a common goal, for instance promote the game. But when you apply changes that impacts members of teams, even though it is for the good of the game, you will get some resistance. For example most clubs are reluctant to release players midyear for "state" clashes. Why? Fear of loosing key players due to injuries. Similarly, even though an incident response process is for the good of a company,

you will run into resistance, mainly as a result of fear of change. Ensure you have "change management" factored into your incident response project. I can't stress enough that establishing an incident response process is as much about writing good process and procedures as it is about managing change within an organisation.

In conclusion, implementing a computer security incident response proved to be more challenging than I had first though. We must remember that it is the people that drive the process, hence the emphasis on documentation should be shared across people change management.

List of References:

- West-Brown, Moira. "Avoiding the Trial-by-Fire Approach to Security Incidents.", Volume 2 Issue 1 March 1999, http://interactive.sei.cmu.edu/news@sei/columns/security_matters/1999/mar/security_matters.htm (June 2003).

- The Office of the Federal Privacy Commissioner, "National Privacy Principles", http://www.privacy.gov.au/publications/npps01.html (July 2003)

- Schultz, Gene. "Forming and Managing an Incident Response Team" Computer Security Journal. Volume XVII (2001): p1-16.

- "Text for ISO/IEC 3rd WD 18044 – Information Technology – Security Techniques – Information Security Incident Management" ISO N3329. Working Draft Text. p1 – 50.

- West Brown Moira, Stikvoort Don, Kossakowski Klaus,Killcrece Georgia, Ruefle Robin, Zajicek Mark, "Handbook for Computer Security Incident Response Teams" 2nd Edition April 2003, http://www.sei.cmu.edu/pub/documents/03.reports/pdf/03hb002.pdf (June 2003)

- Rich, Pethia. "Internet Security Trends", 2001, http://www.cert.org/present/internet-security-trends/sld006.htm (June 2003)

- SANS Institute, "SANS Security Essentials II: Network Security Overview", 2003.

- Zintel, Matthew. "Guidance Software's EnCase Enterprise Provides Incident Response Capabilities Needed to Support Compliance of California Law SB 1386" 2003, http://www.guidancesoftware.com/corporate/News%20Releases/20030414.shtm (July 2003)