Incident Response Planning Using Collaboration Engineering Process Development and Validation

Alanah J. Davis
The Institute for Collaboration Science
University of Nebraska at Omaha
alanahdavis@mail.unomaha.edu

Mehruz Kamal
The Institute for Collaboration Science
University of Nebraska at Omaha
mkamal@mail.unomaha.edu

Terrance V. Schoonover
The Institute for Collaboration Science
University of Nebraska at Omaha
tschoonover@mail.unomaha.edu

Josephine Nabukenya
Institute for Computing and Information Sciences
Radboud University Nijmegen
josephine@cs.ru.nl

Leah R. Pietron
The Institute for Collaboration Science
University of Nebraska at Omaha
lpietron@mail.unomaha.edu

Gert-Jan de Vreede
The Institute for Collaboration Science
University of Nebraska at Omaha
Delft University of Technology, the Netherlands
gdevreede@mail.unomaha.edu

Abstract

Many organizations have plans for incident response strategies. Of particular interest is the fact that an Incident Response Plan (IRP) is not created by a single individual as it requires the inputs and contributions from a range of organizational experts. However, orchestrating the efforts of a group of experts to produce a comprehensive IRP in a short time-frame can be a challenge. Despite IRP being an essential ingredient in conjuring security planning procedures in organizations, extensive literature reviews have revealed that there are no collaborative processes in place for such a crucial activity. This is where the contribution of this study is apparent. This study proposes a design for a facilitated incident response planning process using technology such as group support systems.
(GSS). Three sessions were conducted and an analysis of the sessions revealed that the facilitated IRP process design held up strongly in terms of goal attainment and session participant satisfaction. Future research implications entail devising an all-encompassing integrative general approach that would be applicable to any form of corporate security development planning process.

**Keywords:** incident response planning, contingency planning, collaboration engineering, group support systems

**Introduction**

Driven by the increasing proliferation of e-commerce and e-government, organizations have begun connecting their systems and networks to the outside world. This brings with it special requirements on computer and information security. Most organizations have suffered from security incidents such as viruses and worms, theft of proprietary information, financial fraud, system penetration by outsiders, sabotage of data or networks, to mention but a few. Wack (1991), defines a computer security incident as “any adverse event whereby some aspect of computer security could be threatened; loss of data confidentiality, disruption of data or system integrity, or disruption or denial of availability.”

Organizations today need to have incident response plans in place in order to respond efficiently when an incident occurs. Hence, Incident Response Planning (IRP) is an essential business process for all organizations. IRP is the planning process associated with identification, classification, response, and recovery from an incident (Poindexter, and Laurent, 2000). In a nutshell, IRP involves risk reduction and mitigation and focuses on immediate response.

Despite organizations’ efforts to respond to security risks, extant literature reveals very few guidelines for conducting an IRP. Of particular interest is the fact that an IRP requires the inputs and contributions from a range of organizational experts (Foix, 2004). An IRP is not created by a single individual. However, orchestrating the efforts of a group of experts to produce a comprehensive IRP in a short time-frame can be a challenge. This is where the contribution of this study is apparent. We present a facilitated collaborative process for incident response planning through the use of a collaboration technology, group support systems (GSS). The process design has been applied to three cases and seen to produce the desired results.

In coming up with a collaborative process design that can be executed by practitioners, the following research question needs to be addressed: *How can practitioners collaborate and be more involved in an organization’s contingency planning?* Specifically this research is going to address the area of incident response planning as a start, by asking: *How can IRP practitioners and stakeholders perform/execute a collaborative incident response planning process?* Future research will go beyond incident response and address disaster recovery, business impact, and business continuity in terms of both research and practice. In terms of research into collaborative processes for disaster...
recover, business impact, and business continuity this study presents a comparable collaborative security task. In terms of practice, organizations are more likely to get higher quality IRP without them accessing more resources.

The remainder of this paper is organized as follows. Section 2 gives a background of IRP. The description of our research approach in terms of design and research methods follows in Section 3. The results from the three case studies conducted are discussed in Section 4, and the paper ends with a conclusion and discussion of implications for research and practice in Sections 5 and 6.

**Background**

In order for an organization or business to protect oneself, as a best practice they should establish a contingency plan (Stacey, 2005). Contingency planning is concerned with the development of planned responses to certain disruptive events before they occur (Powanda, et al., 2003). The overall goal of a contingency plan is threefold. The first goal is to minimize the impact of the disruptive event. The second goal is to allow key business activities to move forward in a timely fashion. Finally a contingency plan should be prepared to restore normal operations as quickly and efficiently as possible. A contingency plan is comprised of three elements (Powanda, et al., 2003). As seen in Figure 1 these three elements include: the business continuity plan (BCP), the disaster recovery plan (DRP), and the IRP. Like mentioned earlier, this research deals specifically with the IRP.

![Figure 1: Enterprise Security Planning Model (Excerpted from Powanda, et al., 2003)](image)

Currently there is a significant amount of research in the area of IRP. For example, recently a case study of Egghead.com was reviewed by Polstra (2005). In December of 2000 the internet company suffered an incident involving a hacker. Following the incident, Egghead.com was unable to report to the public whether or not customer credit cards were stolen. Soon after the incident the company filed for bankruptcy. Polstra (2005) concluded that had the company had a well defined IRP in place they would have been able to “weather the storm and stay in business” (pp. 136). Other studies break
down the creation of an IRP and whether or not it proves to be an effective tool for an organization (Rollason-Reese, 2003). However, regardless of the research that can be found in the existing literature, a collaborative process for practitioners to use has not yet been created. Therefore, this research may be a valuable contribution to the field. The following section will further address the elements and stages of an IRP.

IRP is the planning process associated with identification, classification, response, and recovery from an incident (Poindexter & St. Laurent, 2000). In other words, it describes practice of detecting a problem, determining its cause, minimizing the damage it causes, resolving the problem, and documenting each step of the response for future reference. In a nutshell, IRP involves risk reduction and mitigation and focuses on immediate response.

The IRP is usually activated when an incident causes minimal damage, according to criteria set in advance by the organization with little or no disruption to business operations. Incident response planning is also very important because in order to combat incidents, effective incident handling techniques should be employed. Also, it is critical to document all elements of the incident (Poindexter & St. Laurent, 2000).

There are at least six stages of an IRP. They include preparation, identification, containment, eradication, recovery, and follow-up (Poindexter & St. Laurent, 2000). The various stages are outlined in Figure 2.
Figure 2: Procedures for Responding to Computer Incidents (Excerpted from Department of the Navy, 1996)
Understanding each of these stages helps organizations make responding more efficient. It also helps users understand the process of responding so that they can better deal with unexpected incidents. The six stages are detailed here:

1. **Preparation.** This stage is one of the most important stages of IRP. Parties should be prepared to respond before an incident occurs. If parties are not prepared it is more likely that the response efforts will be disorganized and confusion will take over. Preparation can limit the damage potential by making sure the response actions are known and coordinated. This stage also involves the formation of an Incident Response Team (IRT).

2. **Identification.** The identification step is concerned with whether or not an incident has occurred and what the nature of the incident is.

3. **Containment.** The third stage of responding to incidents involves limiting the scope and magnitude of an incident. Incidents involving malicious code can spread rapidly and cause massive destruction and compromise information. This is why containment of the incident is critical.

4. **Eradication.** Eradicating an incident involves removing the cause of the incident. For example, with an incident involving a virus, eradication requires removing the virus from all systems with virus eradication software. A network example would require more work, but the main point is to rid the network of the incident.

5. **Recovery.** This phase involves restoring a system to its normal status. Once the restoration has occurred, it is also necessary to verify that recovery was a success.

6. **Follow-up.** The final stage involves following up on an incident after recovery to help improve incident handling procedures. Often, when an incident is terminated there is little interest in devoting any more attention to the incident. However, this is a critical stage. Following up helps organizations improve their IRP and become more prepared for the next time.

To understand this type of planning process, it is better to look at it from the perspective of what the possible goals might be for an incident response. The goals include confirmation of whether an incident occurred, determining how the attack was done or the incident happened, minimizing the downtime to business and network services, preventing future attacks or incidents, improving security and incident response, enabling legal and law enforcement to prosecute malicious entities, and finally providing recommendations to senior management. Collaboration is important in IRP for a number of reasons. For example, IRP has always been done in a team or with a group of experts; it should only make sense that an efficient process be developed. The next section will discuss our research approach in terms of design and research methods.

**Research Approach**

**Design Method**

The choice for developing a collaborative process design for IRP using a Collaboration Engineering (CE) approach rests on a number of reasons: 1) CE focuses on high-value
tasks, thus organizations will derive maximum benefit from improvements to their highest-value tasks (in this case, IRP) than from improvements to their lower-value tasks (Briggs, Kolfschoten, Vreede, and Dean, 2006) 2) CE seeks to bring the value of facilitated interventions to people who do not have access to facilitation through the creation of repeatable processes (Briggs, Vreede, and Nunamaker, 2003), and 3) designing a repeatable process (in this case a repeatable IRP process) has the possibility of creating intellectual capital for organizations (Vreede, and Briggs, 2005). The key purpose of creating a “repeatable process” following the CE approach is to arrive at a collaborative IRP process that can be applied across organizations. In other words, the process is intended to become a ‘best practice’ for industry rather than being bound to a specific organizational context.

CE has been defined as an “approach for the design and deployment of collaborative technologies and collaborative processes to support mission-critical tasks” (Briggs, Vreede, and Nunamaker, 2003). The main goal of CE is to enable practitioners to work with minimized cognitive load while enabling them with necessary facilitation skills and knowledge about groups. A collaboration engineer is then responsible for designing the process and handing it off to a practitioner in an organization (Kolfschoten, Vreede, Chakrapani, and Koneri, 2006).

In developing an IRP collaboration process design, the key steps involved in the planning process should be converted to patterns of collaboration. Patterns of collaboration are basically a step by step design for a team to achieve its joint task. Patterns of collaboration characterize the way in which a team moves forward to achieve (a part of) its joint task. According to (Briggs, Kolfschoten, Vreede, and Dean, 2006), there are six main patterns of collaboration.

1. **Generate.** Move from having fewer concepts to having more concepts.
2. **Reduce.** Move from having many concepts to focusing on a few concepts deemed worthy of further attention.
3. **Clarify.** Move from having concepts expressed in less detail to having concepts expressed in more detail.
4. **Organize.** Move from less understanding to more understanding of the relationships among concepts.
5. **Evaluate.** Move from less understanding of the value of concepts for achieving a goal to more understanding of the value of concepts for achieving a goal.
6. **Build Consensus.** Move from having less agreement among stakeholders to having more agreement among stakeholders.

These patterns of collaboration are the building blocks with which a CE approach would be utilized in developing an IRP process design. In developing the IRP facilitation process design, the key steps involved in the IRP needed to be converted to patterns of collaboration and finally to specific thinkLets to be executed during the sessions. A thinkLet is the smallest unit of intellectual capital required to create one repeatable, predictable pattern of collaboration among people working toward a goal. Appendix 1 shows the final process design that has been obtained after three iterations of earlier
versions applied in the cases. Appendix 1 outlines the steps necessary for coming up with an IRP, the deliverables from each activity that is carried out, the patterns of collaboration for each step, and the related thinkLets.

The facilitation process model in Appendix 2 depicts the process design. Each of the boxes represents an activity performed during the sessions and specifies the corresponding thinkLet and pattern of collaboration along the top and left-hand side of each box respectively. The deliverables coming out from each activity is shown beside the arrows leading from one box to another.

Research Method

For the development and testing of our collaboration process we followed an action research approach as the basis for the three cases. The action research process proposed in (Zuber-Skerritt, 1991) was followed. This process states that an action research study consists of four phases that can be carried out over several iterations (three in our case): planning, acting, observing, and reacting (Zuber-Skerritt, 1991). The planning phase involves preparation of the research and exploration of the research site. The second phase, act, involves the actual research done by the researchers. The observation phase involves data collection both during the research project and after the research project. Finally, the reflection phase involves analyzing the collected data and forming conclusion which can then be implemented into the next plan phase. After each case, the process of reflection took place in which we would evaluate what did and did not work in terms of the process.

Action research was chosen for this project for a number of reasons. First, it enables us to ask a ‘how to’ research question. One of our goals as researchers is to design something that will improve practice, specifically enabling practitioners to run this process on their own. To do this we asked a ‘how to’ question. Action research also allows us to test something by applying it in a real life setting. What we are trying to design in this case is too complex to test in a lab setting. Further, action research has been successfully used in other similar studies (Koneri, Vreede, Dean, Fruhling, and Wolcott, 2005; Vreede, Fruhling, and Chakrapani, 2005).

Three cases were carried out because this allowed us to reflect on the process design and improve it continuously. The following cases were carried out:

- **Case 1**: Student Lab Computer Incident Response Plan with 17 students enrolled in an undergraduate level information security course.
- **Case 2**: Student Lab Computer Incident Response Plan with ten students enrolled in a graduate level information security course.
- **Case 3**: Employee Workstation Incident Response Plan with a combination of eight computer professionals and information systems faculty at a university.

The task asked the participants to create an IRP that specifically develop the course of action (COA), team member responsibilities, and documentation and logs that should be
tracked in the case that a certain incident should occur. The actual incidents in the task included viruses and worms, trojan horses, denial of service attacks, root kits, and spy ware and ad ware. The category of COA called for actions to be entered that would be taken to address computer failure due to the incident type. The team member responsibilities called for ideas on what responsibilities need to be assigned to people and in place in order to deal with the incident (i.e. any special skills that may be needed). Finally, the documentation and logs category called for facts to be entered that should be recorded about the incident such as the program, operating system, et cetera. In each case the group used a GSS as a collaborative platform to produce an complete IRP.

Research data was collected from multiple sources in order to enable rich understanding and comparison and contrast. Table 1 below makes explicit the data sources that were used:

<table>
<thead>
<tr>
<th>Sources for Data Collection</th>
<th>Description</th>
</tr>
</thead>
</table>
| Direct Observation | Using a pre-defined observation instrument researchers made notes of:  
- critical incidents  
- questions from participants relating to the workshop process  
- questions from participants relating to workshop content |
| Online Feedback | Participants were asked a series of open-ended questions in GSS about:  
- likes about the workshop experience  
- dislikes about the workshop experience  
- suggestions for the workshop experience  
- other general comments |
| Questionnaires | Participants completed a survey about meeting satisfaction based on (Briggs, Reinig, and Vreede, 2006). |
| Data Logs from the GSS or session data | The session data was the actual IRP consisting of the contributions that the participants in each of the three cases made online into the GSS. |
| Informal Interviews | Interviews were held with a few subject matter experts in order to get a better understanding of their perceptions of the IRP process. |

Table 1: Data Sources

The research data contributed to the reflect stage of action research. Based on the analysis of the data after each case, continuous improvement of the design was done. The analyses of the data from the multiple sources listed in Table 1 was done collaboratively by the researchers. A shared understanding of the interpretation of the data was reached through a process of discourse among the group of researchers involved in this study.

The researchers functioned as a team with shared responsibilities in all aspects of the study. In particular, during the ‘act’ phases of the three cases (i.e. the workshops with the participants) responsibilities were divided as follows:

- **Presenter.** One researcher presented the goal, agenda, context, GSS technology, and starting considerations to the participants.
- **Facilitator.** One researcher moderated the participants’ intentions to execute the IRP process.
- **Chauffeur.** In each workshop, one researcher operated the master console of the GSS environment. The GSS used was *GroupSystems™ Workgroup Edition 3.4.*
- **Observer.** One researcher exclusively focused on making detailed observations using the observation instrument described above. In addition, each member of the research team kept observation notes whenever possible during the workshop. After each workshop, all researchers captured further observations that came to mind, inspired by the observation instrument.

The assignment of roles to researchers varied from case to case. The roles of presenter, facilitator, chauffeur, and observer were rotated in the team. It is also important to note that the researchers were inexperienced as facilitators which made them more like IRP “practitioners” and hence functioned as representative “test subjects.” Additionally, one member of the research team functioned as a subject matter expert that would answer the researcher’s questions regarding incidents and response plans. Researchers were not remunerated for their services by any of the groups that participated in the study. It should also be noted that the researchers did not intervene in the actual content of the workshops, other than by clarifying issues when so prompted by participants.

**Results**

In this section our results have been separated into design results which discuss the results of the IRP in a quantitative way and application results which discuss the results of the IRP in both a quantitative and qualitative way.

**Design Results**

As mentioned earlier, three cases were used to test the collaboration process design for the creation of an IRP. Tables 2 and 3 show the number of contributions, unique contributions, and off-task comments given in both the divergence (i.e. the generation of course of action steps, team member responsibilities, and documentation steps that should be taken for each incident) and convergence (i.e. the merging and consolidation of ideas into a finalized IRP) tasks. Unique contributions are defined as contributions under the same heading that expressed dissimilar ideas. Off-task contributions would many times tend to be a humorous comment that added no significant contribution to completing the task. More specifically, Table 2 gives the results of the original brainstorming and idea generation session while Table 3 gives the results of the clean-up of those ideas into a workable IRP document.

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Total</strong></td>
<td>156</td>
<td>158</td>
<td>172</td>
</tr>
<tr>
<td>Contributions per stakeholder</td>
<td>9.18</td>
<td>15.80</td>
<td>21.50</td>
</tr>
<tr>
<td>Unique</td>
<td>144</td>
<td>151</td>
<td>170</td>
</tr>
<tr>
<td></td>
<td>92.31%</td>
<td>95.57%</td>
<td>98.84%</td>
</tr>
<tr>
<td>Contributions per participant</td>
<td>8.47</td>
<td>15.1</td>
<td>21.25</td>
</tr>
<tr>
<td>Off-task</td>
<td>3</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>1.92%</td>
<td>0.63%</td>
<td>0.0%</td>
</tr>
<tr>
<td>Contributions per participant</td>
<td>0.18</td>
<td>0.10</td>
<td>0</td>
</tr>
</tbody>
</table>

Table 2: Contributions from brainstorming activity
### Application Results

The final output from the teams in each case resulted in a useable IRP. Figure 3 presents the course of action in response to virus and worm incidents that was delivered in Case 3.

1. First step: Disconnect the infected host from LAN/WAN to prevent propagation.
2. Second step: Capture system state and observed symptoms. This includes: (1) User-observed symptoms in timeline context (what happened when in connection to what activities); (2) Host system state (O/S version, patches, registry/config-files, etc); antivirus version and signatures); and (3) Network/gateway logs (traffic logs, etc.). This may include scanning the system with other antivirus products and/or updated signatures.
3. Third step: Use the results of step 2 and external sources (like AV vendor, CERT, etc) to characterize the virus/worm/trojan and its attributes (including recovery methods).
4. Fourth step: Prepare to recover the infected host. This uses pre-determined checklists/templates.
5. Fifth step: Recover the infected host to known good state.
6. Sixth step: Update protective/detective mechanisms at host, antivirus gateway, firewall, ISP filters, etc.
7. Seventh step: Restore service, including network connectivity, to recovered host.
8. Note: If infection is novel (e.g., 0-day), may need to recreate vulnerable state on a test bed host to determine effectiveness of protective/detective updates before connecting operational hosts to network.

![Figure 3: Case 3 Course of Action deliverable for virus and worms](image-url)

Additionally, the General Meeting Assessment Survey questionnaire (Briggs, Vreede, Reinig, 2006) was used in order to judge the participants’ satisfaction with the process and its outcomes. For details regarding the theoretical underpinning and validation of this instrument, see (Briggs, Reinig, and Vreede, 2006). This tool uses 7-point Likert scale questions, ranging from strongly disagree to strongly agree. The compound results of the questionnaire are shown in Table 3.

<table>
<thead>
<tr>
<th>Satisfaction with Process</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Score</td>
<td>4.850</td>
<td>4.210</td>
<td>4.363</td>
</tr>
<tr>
<td>Standard Deviation</td>
<td>1.306</td>
<td>1.670</td>
<td>1.101</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Satisfaction with Outcome</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Score</td>
<td>4.376</td>
<td>4.335</td>
<td>4.300</td>
</tr>
<tr>
<td>Standard Deviation</td>
<td>0.913</td>
<td>1.282</td>
<td>1.666</td>
</tr>
</tbody>
</table>

Table 3: Satisfaction with process and outcome
At the end of each study, participants were asked to enter any positive and negative comments that they wished to make concerning the session. Typical positive comments received from the three pilot sessions included “it was an interesting concept to help produce large quantities of brainstorming ideas”, “liked the anonymity…it made it easy to have an open forum of input” and “it was easy to make quick revisions”. Most of negative comments had to do with the way that the study was done, such as “need to spend more time on instructions” and “provide help to those who are confused”. These issues were corrected in subsequent sessions.

One comment made by all three groups was the lack of sufficient time to adequately cover the topic. It was found that as the expertise of the three groups improved, (from undergraduates to graduates to professionals and faculty), time became a critical factor in their ability to enter all and properly discuss all of the aspects of IRP that they felt should be included.

Aside from the reported lack of time, the results of the study and the feedback received from the participants support the conclusion that they were satisfied with the process and found the workshops to be useful. From the researcher/developer perspective, the participants seemed very comfortable with the GSS technology, which made execution easy.

**Conclusion**

As has been discussed earlier, having a successful contingency plan in place is paramount to the minimization of damage from an information security incident. There has, however, been very little research done on the development of such a plan. In looking at this problem, it becomes apparent that for a workable plan to be developed, the expertise from a number of systems and security personnel within the organization needs to be accessed. Their ideas and comments need to be grouped and organized so that a workable plan emerges.

The focus of this study was to design and test a collaborative process for the creation of an IRP that would be both workable and repeatable. This was done using an iteration process based on the feedback from three case studies. The results of the three cases suggest that the process indeed has the potential to support organizations in creating useful IRPs. The consensus of both the participants and the subject matter expert along with the qualitative and quantitative results reported previously lead us to believe that the process was successful and could accomplish the goal of developing a workable IRP. By testing it using three distinct groups of subjects, the results also support the idea that the designed process can be applied in different organizational contexts.

Some issues emerged that should be taken into account for future research and the organizational application of the process. The fact that there was relatively little difference between the total number of contributions and the number of unique contributions leads us to believe that the participants could have used more time to effectively complete all that needed to be accomplished. Their feedback, both in
responses to the open questions in the GSS and during the interviews, lends support to this observation. On the other hand, the combination of high rate of contributions and low rate of off-task comments gives us reason to believe that this process was successful in obtaining the goal of keeping people on task and working towards the given task. Consequently, this shows a level of efficiency in the use of resources.

This study paves the way for organizations to use collaborative processes and facilitation techniques to develop an IRP specific to the needs of their operation. Using such concepts as collaboration, iteration, anonymity, and voting, many ideas can be generated and consolidated in a relatively short period time, producing a workable plan specific to the needs of the particular enterprise.

**Implications for Research and Practice**

Organizations need to have an IRP in place to minimize the impact of a disruptive event, to allow key business processes to move forward in a timely fashion, and to restore normal operations as quickly and as efficiently as possible. Traditionally, compiling an IRP within an organization has been a process involving more than one person collaborating through manual discourse. The manual process translates into valuable business time consumption and gives rise to environments where participants of the task are not always able to express their candid opinions due to power structures present in the organization. In other words, participants responsible for drawing up an IRP might have differing hierarchical roles and someone lower in the hierarchy might back-out from openly expressing their thoughts in front of their senior colleagues. This concern may be erased with the approach presented in this study. Our proposed approach highlights an inherent property of the GSS system and an important implication for practitioners, which has to do with anonymity. Anonymity will enable the gaps present due to official hierarchies to be erased and a more balanced input from all IRP planners to take place resulting in a comprehensive plan.

The aim of this study was to design and test a collaborative IRP process following the CE approach. To this end, we refined a collaboration process design in three iterations using feedback from observations, surveys, and interviews. The process provides IRP practitioners and stakeholders with the tools to prepare an incident response plan that includes 1) the identification of the incident, 2) the notification of appropriate authorities, 3) the containment of the incident, 3) its eradication, and 4) the recovery from the incident. Another important implication to highlight for this study is the process of conducting a follow-up plan to analyze the incident response that was carried out in tune with the IRP and to suggest any modifications to the existing IRP. Such sessions can be easily implemented with our proposed process by simply altering the taxonomy of incidents to comprise of issues that need to be modified.

One of the most important implications for practice is the fact that the planning process suggested in this study can be conducted by an employee within an organization by simply following the steps in the process design. This would then eliminate the need to hire external facilitators to conduct the sessions. This has a number of direct impacts such
as limiting organizational monetary resources that would have been used to pay the facilitator and also limiting the risk of proprietary information being leaked outside organizational boundaries.

The results of our study open various avenues for future research. First, considering this was an exploratory study, there are many opportunities to expand and refine this work. Our proposed incident response planning design needs to be validated – both internally & externally - in the real-world context of organizations across diverse industries to see if the design can be truly generalized. Our next major research milestone would be to develop similar planning processes for other security planning areas such as disaster recovery, vulnerability assessment, business continuity, and risk assessment planning. And we are hopeful of expanding this research to eventually design an all-encompassing enterprise security planning process whereby a single approach can be applied to produce a comprehensive security plan addressing all aspects of an organization’s defense mechanisms.

References


Appendices

Appendix 1: Process Design

<table>
<thead>
<tr>
<th>Steps</th>
<th>Deliverables</th>
<th>Patterns</th>
<th>ThinkLet</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Agreeing on the taxonomy of incidents.</td>
<td>Consensus on the list and definitions of incidents</td>
<td>Consensus Building</td>
</tr>
<tr>
<td>2.</td>
<td>Get input on categories under each incident. a) Course of action b) Team member responsibilities c) Documentation</td>
<td>Items to be considered in each of the categories</td>
<td>Generate</td>
</tr>
<tr>
<td>3.</td>
<td>Clean up the category lists.</td>
<td>Non-redundant and well-framed ideas in each category</td>
<td>Reduce</td>
</tr>
<tr>
<td>4.</td>
<td>Read comments cleaned up by other participants in sections other than yours. Make any comments that you feel need to be addressed in those sections.</td>
<td>Reviewed list of incident categories by all session participants</td>
<td>Generate</td>
</tr>
<tr>
<td>5.</td>
<td>Go back to your own assigned incident and read what others have commented on. Incorporate feedback to improve your section.</td>
<td>Categories with feedback incorporated</td>
<td>Reduce</td>
</tr>
<tr>
<td>6.</td>
<td>Reach consensus on the items entered in the categories.</td>
<td>A final agreed upon list of ideas for each type of incident</td>
<td>Vote Consensus</td>
</tr>
<tr>
<td>7.</td>
<td>Wrap-up</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Appendix 2: Facilitated IRP Process Flow Chart