Collaboration Engineering For Incident Response Planning: Process Development and Validation

Mehruz Kamal[1]
mkamal@mail.unomaha.edu

Alanah J. Davis[1]
alanahdavis@mail.unomaha.edu

Josephine Nabukenya[2]
josephine@cs.ru.nl

Terrance V. Schoonover[1]
tschoonover@mail.unomaha.edu

Leah R. Pietron[1]
lpietron@mail.unomaha.edu

Gert-Jan de Vreede[1,3]
gdevreede@mail.unomaha.edu

[1]*The Institute for Collaboration Science, University of Nebraska at Omaha*
[2]*Institute for Computing and Information Sciences, Radboud University Nijmegen*
[3]*Delft University of Technology, the Netherlands*

Abstract

Many organizations have plans for incident response strategies. Despite Incident Response Planning (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 study proposes a design for a facilitated incident response planning process using technology such as GSS. Three sessions were conducted and an analysis of the sessions revealed that the facilitated IRP process design held up strongly in terms of efficiency, 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.

1. Introduction

Today, many organizations have connected their systems and networks to the outside world (e-business). 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 in [10], 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 need to have incident response plans in place to be able 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 [8]. 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. Processes are in place that may assist security planners within organizations to plan for such events. Of particular interest is the fact that an IRP requires the inputs and contributions from a range of organizational experts. 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, GSS. The process design has been applied to three cases and seen to produce the desired results.

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 [2], 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 [1], and 3) designing a repeatable process (in this case a repeatable IRP process) has the possibility of creating intellectual capital for organizations [10]. 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.

In coming up with a collaborative process design for incident response planning that is predictable, repeatable, and that can be executed by practitioners, the following research question had to be addressed: *How can IRP practitioners and stakeholders perform/execute a collaborative incident response planning process?*

1530-1605/07 $20.00 © 2007 IEEE

The remainder of this paper is organized as follows. Section 2 gives a background of CE. The description of our research approach and process design follows in Sections 3 and 4. The results from the three case studies conducted are discussed in Section 5, and the paper concludes with a discussion of implications, and future research directions in Sections 6 and 7.

2. Background

CE has been defined as an "approach for the design and deployment of collaborative technologies and collaborative processes to support mission-critical tasks" [1]. 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 [6].

Figure 1 shows the CE approach for the design of collaboration processes. According to [6], there are six steps in the approach which are executed in incremental/iterative, non linear fashion:

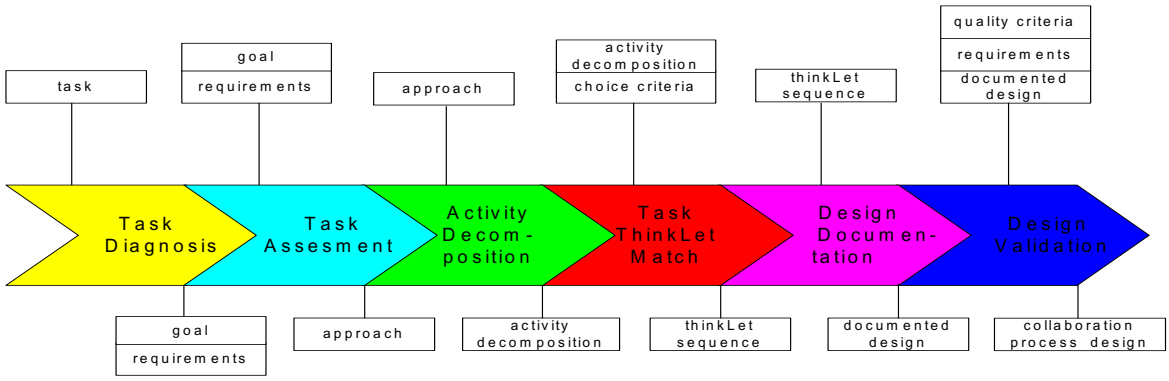

Figure 1: Design approach (Excerpted from [6])

1. *Task Diagnosis*. The first step involves interviews with the problem owner in order to identify the problem and the goal of the collaboration process. In our research, we met with IRP subject matter experts in order to complete this step.
2. *Task Assessment*. During this step, the process to complete the task should be determined. In our case there was not an existing process available, this was the first of its kind. Therefore, we began by listing all of the deliverables and the activities necessary in order to accomplish each.
3. *Activity Decomposition*. This step refers to the six patterns of collaboration, see below [2]. The decomposition of the activities from the previous step should stop when each step cannot be decomposed any further in terms of the patterns of collaboration.
4. *Task-ThinkLet Match.* Once the activities have reached the lowest level of decomposition they are matched with thinkLets. A thinkLet is the smallest unit of intellectual capital required to create one repeatable, predictable pattern of collaboration among people working toward a goal [1]. See Table 1 in section 4 for our results of the above steps.
5. *Design Documentation*. The design documentation is the document that would be handed off from the collaboration engineer to the organization practitioner. The document includes the problem and process description, detailed agenda, and a facilitation process model. The facilitation process model visualizes the sequence of thinkLets and the process flow decisions that have to be considered during the execution of the collaboration process.
6. *Design Validation*. Finally, there are four ways to validate a design; pilot testing, walk through, simulation, or review. In our case, we used a combination of pilot testing (3 cases), walkthroughs, and reviews. Each validation activity led to improvements in the process design.

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 characterize the way in which a team moves forward to achieve (a part of) its joint task. According to [2], 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.

3. Research Approach

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 [12] 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 [12]. 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 reacting 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 ([7], [5], [9]).

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.

For each case, the meetings had two goals. The primary goal for the meeting participants was to experience how teams come together in order to build an incident response plan. The secondary goal for the meeting participants was to see how collaboration technology (GSS) can be used to accomplish the main goal. The purpose of the workshops from the researcher's perspective was to design and evaluate a collaborative IRP process that is repeatable, predictable, and can be executed by practitioners.

The purpose of the workshops from an IRP perspective was to produce a useable incident response plan. The first case had a group size of 17 undergraduate students including 16 males and one female. The second case had a group size of ten graduate students including eight males and two females. The final case had a group size of eight professionals including seven males and one female. The nature of the participants in terms of their background knowledge and expertise differed among the three cases. In the first case the students were enrolled in a course called "Information Security and Policy." In the second case the students were enrolled in a course called "Strategic Planning Information Assurance." In the final case the workshop participants included a combination of security professionals and academics in the area of security. In all cases the workshop participants had minimal background with technology supported collaboration processes. Each workshop lasted about an hour and a half.

Research data was collected from multiple sources in order to enable rich understanding and comparison and contrast. The following sources were used:

1. Direct Observation. Throughout each workshop, researchers made notes of critical incidents and questions from participants relating to the workshop process and content. (e.g., one participant asked: "Can I discuss with the person next to me for this activity") Observations were also made relating to a number of pre-defined aspects e.g. 1, 2, 3. The pre-defined aspects were listed in an observation instrument.

2. Online Feedback. At the end of each workshop, participants were asked to respond to a series of prompts in GSS. These prompts represented open ended questions that solicited participants to enter their likes and dislikes about the workshop experience and offer suggestions and other comments.

3. Questionnaires. After each workshop, participants were asked to fill out a brief questionnaire that captured information about meeting satisfaction. This instrument is based on [4].

4. Data Logs from the GSS or session data. The results of each group session were stored electronically. These consisted of all the contributions that the participants in each of the three cases made online into the GSS. These contributions provided insights into the focus and clarity of the assignments that were given by the facilitators to the participants and the usefulness/clarity of the tools.

5. Informal Interviews. Interviews were held with a few subject matter experts. The interviews were held after each session in order to get a better understanding of the success of the process.

The direct observation, online feedback, session data, and informal interviews all contributed to the reflect stage of action research. The conclusions that were drawn from these data sources were taken into consideration when the next case was to be executed. The results from the questionnaires were compiled in an Excel spreadsheet in order to compute the averages and standard deviations in terms of contributions and survey results. This also allowed for comparison among the respondents. Based on the analysis of the data after each case, continuous improvement of the design was done.

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, and starting considerations to the participants. The presented also handled questions about the focus and process. Finally, the presenter also guided the warm-up exercise to get the participants acquainted with the GSS.
- *Facilitator*. One researcher guided the participants through activities to execute the collaborative IRP process. Responsibilities included, but were not limited to: explaining each agenda activity, giving assignments, guiding discussions, and keeping track of time. The facilitator executed the process through the use of the thinkLets, see Section 4 for more details.
- *Chauffeur*. In each workshop, one researcher operated the master console of the GSS environment. The GSS used in the studies was *GroupSystems*™ Workgroup Edition 3.4. The chauffeur's responsibilities included starting and stopping the participants' tools on their screen, moving or modifying contributions, and assisting with technical issues.
- *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. As the study was also a learning experience for part of the research team, it was ensured that 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.

4. 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. Table 1 shows the final process design that has been obtained after three iterations of earlier versions applied in the cases. The actual process design that was utilized for each of the cases is a condensed version of the one shown in Table 1 (see Appendix). Table 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.

For each of the steps 1 to 6, following is a description of how they match with a pattern of collaboration and a related thinkLet. Step 7 is a wrap-up activity that entails distributing a survey questionnaire to the participants to obtain their level of satisfaction with the process as well as asking them to answer a few process related questions through the GSS system.

(i) *Step 1*: In this step, the session participants are given the definitions of the incidents (viruses and worms, Trojan horses, denial of service, root kits, spyware, & adware) and are asked whether they agree with the presented definitions. Feedback regarding the definitions is taken into consideration and changes are made to the taxonomy before moving onto the next activity. This activity translates to "building consensus" among the group members and is achieved through the "Turn Taker" thinkLet. This is a simple thinkLet that allows each participant to, in turn, verbally express their agreement with the taxonomy presented.

(ii) *Step 2*: This step translates into the "generate" pattern of collaboration. The related thinkLet for this activity is the LeafHopper. This thinkLet is usually applied when the team must brainstorm on several topics at once and also when different participants will have different levels of interest or expertise in different topics. This thinkLet is ideal for situations where it is not important to assure that every participant contributes to every topic. Applying this particular thinkLet will help foster broad participation and synergy during the population of the taxonomy of incidents with rough contributions. The expected output from this activity is a list of contributions categorized as Course of Action (COA), team member responsibilities, and documentation for each of the five incident types.

(iii) *Step 3*: In this step, participants are assigned to teams of two to three people to work on each of the incident categories. The teams review all the comments that were entered into their categories and attempt to remove

redundant ideas and come up with structured sentences. This activity mimics the "reduce" pattern of collaboration. The related thinkLet for this step is the BucketSummary. This thinkLet involves removing redundancy and ambiguity from comments in categories. The inputs for this thinkLet are categories containing unedited brainstorming comments and the outputs are categories containing concise, non-redundant, unambiguous sentences, paragraphs, or lists.

Table 1: Final Process Design

Steps	Deliverables	Patterns	ThinkLet
1. Agreeing on the taxonomy of incidents	Consensus on the list and definitions of incidents	Consensus Building	Turn Taker
2. Get input on categories under each incident a) Course of action b) Team member responsibilities c) Documentation	Items to be considered in each of the categories	Generate	LeafHopper
3. Clean up the category lists	Non-redundant and well-framed ideas in each category	Reduce	BucketSummary
4. 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.	Reviewed list of incident categories by all session participants	Generate	LeafHopper
5. Go back to your own assigned incident and read what others have commented on. Incorporate feedback to improve your section.	Categories with feedback incorporated	Reduce	BucketSummary
6. Reach consensus on the items entered in the categories	A final agreed upon list of ideas for each type of incident	Vote Consensus	StrawPoll CrowBar
7. Wrap-up			

(iv) *Step 4*: This step involves a read-comment cycle. In this activity, each sub-team of two to three people are asked to read the cleaned up entries in other incident categories than their own and make any comments on issues they feel need to be addressed. This activity once again applies the LeafHopper thinkLet as was done earlier in step 2.

(v) *Step 5*: Once the participants have reviewed the other categories, they are asked to return to their own assigned incident category and read what the rest of the group have commented on. Then they incorporate the feedback into their sections. This activity ensures that any gaps that might have been overlooked by the assigned incident teams can be brought to light by the other session participants. This step involves the BucketSummary thinkLet described earlier in step 3.

(vi) *Step 6*: This step actually involves two parts. The first one is to take a vote on the incidents to see if all session participants agree and then carry out discussions and any related modifications to existing categories that received high percentage of disagreement as revealed by the voting results. These activities translate to evaluation and building consensus patterns of collaboration. The related thinkLet for evaluation is the StrawPoll. This thinkLet allows participants to obtain a feeling of the group's position by casting votes and reviewing results. This is done primarily to initiate a discussion rather than to end it. As a result, the outputs from the StrawPoll is a tabular and graphical display of the patterns of consensus in the group. The voting activity is conducted in the following manner. Each participant is given a voting ballot sheet. They are asked to once again read through all the incident categories and write down their votes as either a "Yes" – meaning the category is adequately covered, or a "No" – meaning the category is not adequately covered on the voting sheet. The voting ballot sheet also has space provided to allow session participants to jot down any notes as they read through each incident category for further discussion at a later time. Once everyone has completed reviewing all incident categories, the group is then requested to cast their votes in GSS. The second part of this step is the process of building consensus. This will be achieved by the CrowBar thinkLet. CrowBar allows the group to address the reasons for a lack of consensus on certain issues. This thinkLet enables the participants to engage in a structured anonymous discussion of the items that showed the highest percentage of disagreement over the set of scores. The key output from conducting the Crowbar is a shared understanding of the reasons behind differences of opinion within the group.

The facilitation process model in figure 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.

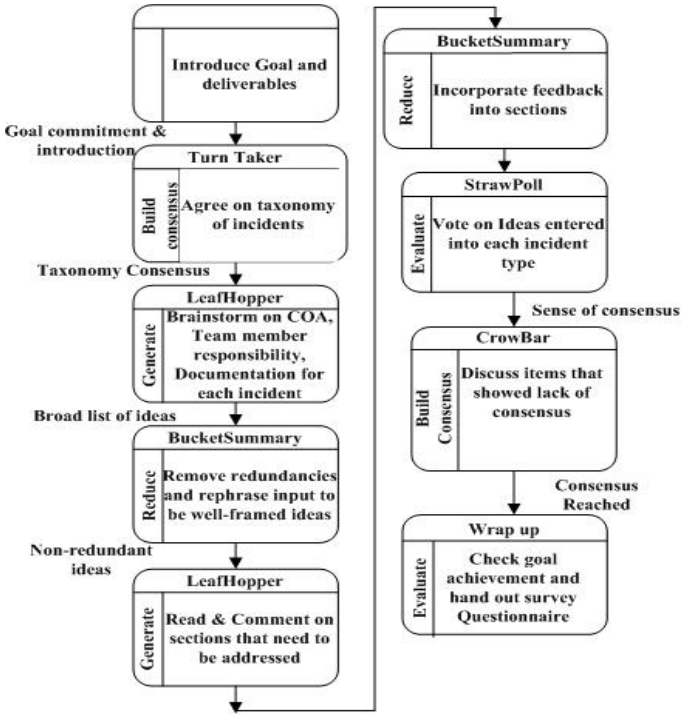

Figure 2. Facilitated IRP Process Flow Chart

4.1. Process Design Refinement

The final process design shown in Table 1 is a product of three refinement iterations. We briefly highlight some of the areas that have been modified since the initial process design.

Step 1 involves obtaining consensus on the pre-determined taxonomy of incidents with all participants in the session. The initial set of taxonomy included "hacking utilities" as an incident type. This was later removed from the final design and replaced by "root kits." Another change worth mentioning is the merging of the two separate incident types, "viruses" and "worms" as one incident type. This was done with the consideration that session participants would tend to enter similar and redundant entries in these two incident types. So to minimize redundancy of data, these two incidents were combined into one. It is important to note that the cases carried out for the study outlined here all involve a taxonomy of electronic incidents. This same process can be applied to other incident response planning programs regardless of the nature of the incidents in the taxonomy.

Step 3 is the process of cleaning up the ideas obtained from brainstorming in step 2. The process design for this step has changed from the initial design (see Appendix) in terms of assigning people to work on specific incidents just before the clean-up activity and not before the brainstorming activity. The reason for the change was to maximize the potential to obtain a broader range of contributions from all participants during the brainstorming phase as well as to have people pair up before the clean-up activity to have a directed focus on a specific incident category.

Steps 4 and 5 in the final design are a completely new addition from the initial design (Appendix). These steps have been incorporated to improve the likelihood of reaching consensus among group members to assure that each of the incidents and its constituent sub-categories have been adequately covered and there are no missing issues to be addressed in any of the sections.

Step 6 (step 4 in initial design, see Appendix) has remained constant throughout the designs and is involved with going through all categories of ideas and voting to check consensus with the group.

Step 5 from the initial process design (see Appendix) was involved with determining severity levels to apply to each incident. This step has been eliminated from the final design process due to the fact that in reality, one must deal with any and all incidents that occur. It is highly unlikely that prioritization of the incidents will be necessary.

4.2. Assumptions

At this point it is important to highlight some of the assumptions we made in carrying out our incident response facilitation process. The first one being that the entire process was an iterative one. What this means is that running through the whole session – beginning with brainstorming ideas to voting on results to reaching consensus – might not bring about full agreement among group members in one iteration. A number of rounds of discussions and consensus building might be needed that might go beyond the time frame allotted for the session. The assumption here is that the researchers as well as the participants understand that the process flow of the session allotted for the one and a half hours is just the first step in reaching the goal of coming up with an incident response plan through facilitation using GSS.

4.3. Preparation

A number of preparation steps have to be carried out before an actual IRP facilitation session can be executed. The first and foremost task that needs to be carried out is formulating the task agenda. The agenda outlines the activities as well as the duration of each of the activities that the group will carry out during the entire session. The task agenda is entered both on a slide to present to the groups as well as into the groupware system so that it is all ready to go when the session begins.

It is important to note here that for each of the three cases, steps 4 and 5 had to be left out to fit the time

allotted for the sessions. The introduction and warm-up exercise is allotted 15 minutes. The brainstorming activity is conducted for 20 minutes. Step 3 which involves the clean-up activity is allotted 25 minutes. Voting and reaching consensus is allocated 20 minutes. Finally, the wrap-up activity is carried out for 15-20 minutes. All three sessions are conducted over a period of one and a half hours and care and attention is taken to ascertain that there is room for flexible facilitation: the facilitator is alert as to the progress of each of the activities and attention span of the session participants and adjusts the allotted time for specific activities accordingly.

The next preparation step involved coming up with thorough definitions of pre-determined incidents. The definitions for the three cases were obtained from the Federal Communications Commission Computer Security Incident Response Guide as well as other existing security literature. It was agreed on by the research team that a warm-up exercise needed to be designed to allow the session group participants to try out GSS before getting fully immersed in the actual task activity. The warm-up activity was designed utilizing the same groupware tools that would be used during the actual IRP brainstorming activity.

A major step towards preparing for the sessions is the setup of the facility. Facility setup is scheduled to be carried out on average two hours before the sessions began. The instruments involved in the setup comprise of laptops, network cables, power cords, hubs, LCD projectors, two projection screens, and of course tables and chairs. The tables were laid out in a horse-shoe pattern facing outwards toward the two projection screens. Prior experience shows that for group sizes ranging from 5 to 15 people, a horse-shoe arrangement is ideal. This type of layout enables the group members to see each other and helps create an environment where directed discussions among members can take place. From the perspective of the facilitator, a horse-shoe pattern allows him/her to be able to walk around the room to assist and view the progress of the session easily without disrupting participant activities. A white sheet of paper is placed with each laptop to allow session members to write down any comments or thoughts they might have during the session. In addition to that, name tags are also placed at each sitting location. This is done to create a more personal atmosphere so that the facilitator would be able to refer to participants by name and thus ease interactions with members.

5. Results

As mentioned earlier, three cases were used to test the collaboration process design for the creation of an IRP. During the sessions, we monitored participants' perceptions along with the efficiency and effectiveness of the process in achieving the preset goals of the collaboration process. We analyzed the process along the four constructs: productivity, efficiency, effectiveness, and user satisfaction.

Tables 2 and 3 show the number of contributions, unique contributions, and off-task comments given in both the divergence and convergence tasks. Table 2 gives the results of the original brainstorming session while Table 3 gives the results of the clean-up of those ideas into a workable format.

Table 2. Contributions from brainstorming activity

Divergence	1	2	3
Total	**156**	**158**	**172**
Contributions per stakeholder	**9.18**	**15.80**	**21.50**
Unique	**144 92.31%**	**151 95.57%**	**170 98.84%**
Contributions per participant	**8.47**	**15.1**	**21.25**
Off-task	**3; 1.92%**	**1; 0.63%**	**0; 0.0%**
Contributions per participant	**0.18**	**0.10**	**0**

Table 3. Contributions from clean-up activity

Convergence	1	2	3
Total	**134**	**139**	**182**
Contributions per Stakeholder	**7.88**	**13.90**	**22.75**
Unique	**132 98.51%**	**136 97.84%**	**182 100%**
Contributions per Participant	**7.76**	**13.60**	**22.75**
Off-Task	**10; 7.5%**	**0; 0.0%**	**0;0.0%**
Contributions per Participant	**0.59**	**0.0**	**0**

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.

5.1. Productivity

Productivity is defined as the outcomes achieved over the resources used in a collaboration process in order to arrive at satisfactory results. To measure group productivity, we used the number of contributions, and the uniqueness of contributions made. We also looked at the number of off-task comments that were made.

Despite the limited time of 15 to 25 minutes given to each activity, the number of total and unique contributions was substantial (Table 3). It is also interesting to note that as the study was refined, the number of total and unique contributions per participant increased dramatically. This can also be attributed to the nature of the participants (the third case comprised of security academics and professionals).

5.2. Efficiency

Efficiency is the resources used as compared to the resources planned for a particular action. To measure perceived collaboration process efficiency, we determined how well participants understood the process/task and could execute it within the planned time limit.

From our observations it followed that the process was fairly efficient. For example, we had about 100 contributions after about 15 minutes in one of the workshops. In total, it took the participants about an hour and a half in each workshop to execute the process.

5.3. Effectiveness

We define this construct as the extent to which participants meet the process goal. We measured the extent to which participants met the process goal. From the researcher/developer perspective, the participants managed to arrive at satisfactory results.

It should be noted, however, that some participants questioned both the goal and the process because of failure to reach consensus at some point in one of the workshops. This was due to the fact that an iterative process of goal refinement and consensus could not be done in the allotted time.

5.4. User Satisfaction

We define this construct as an effective response with respect to the attainment of goals [4]. In order to judge the participants' satisfaction with the process and its outcomes, the General Meeting Assessment Survey questionnaire [4] was used. For details regarding the theoretical underpinning and validation of this instrument, see [3] 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 4.

Based on the results shown and the feedback received, the participants were undoubtedly satisfied 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.

Table 4. Satisfaction with process and outcome

Satisfaction	1	2	3
Satisfaction with Process			
Score	**4.850**	**4.210**	**4.363**
Standard Deviation	**1.306**	**1.670**	**1.101**
Satisfaction with Outcome			
Score	**4.376**	**4.335**	**4.300**
Standard Deviation	**0.913**	**1.282**	**1.666**

After analyzing the comments made by the participants, the reason for the decrease in scores of the three groups became apparent. As the expertise of the three groups improved, (from undergraduates 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.

6. Discussion

The primary focus of this study was to design a transferable, repeatable, and predictable collaboration process for the creation of an IRP. This process was designed and tested in three case studies. The process proved to be fairly productive: the participants generated 144 to 170 contributions on average in each case. Yet, the three cases only represent first field test of the process. A number of issues emerged that have to be taken into account for future tests and the organizational application of the process.

First, the high rate of contributions, along with the low rate of off-task comments give us reason to believe that this process was successful in obtaining the goal of keeping people on task and working towards the given task. However, it appeared that there was relatively little difference between the total number of contributions and the number of unique contributions. This leads us to believe that the participants did not have enough 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.

Second, it appears that the designed process can be applied in different organizational context to craft an IRP collaboratively. The only element of the process that is dependent on the context in which it is applied is the taxonomy of incidents. This can be fine-tuned to each situation. During the course of the three cases, the taxonomy was modified once without impacting the rest of the process or its execution. Also the subject matter experts in the third case supported the notion of the broader contextual applicability of the process during the informal interviews.

Third, the results of the three cases suggest that the process indeed has the potential to support organizations in creating useful IRPs. The subject matter expert

acknowledged that in each case the participants created useful material that could have been easily incorporated into a full-fledged IRP. Time constraints prevented us from having the groups finalize any of the IRP plans but there was fairly broad consensus that the workshops resulted in very useful elements that could be readily used.

Fourth, from a research perspective, this study consciously followed the Collaboration Engineering design process as defined in [6]. The experiences during the study confirm the applicability of the various design steps. However, the experiences also stress the need for iteration and incremental steps during the design of repeatable collaboration processes. The action research approach to conducting this study appears to be congruent with the nature of the Collaboration Engineering design process. It appears to be hard to get a repeatable process 'right the first time'. Also, working in a number of pilot cases allowed us to focus special attention to certain elements in the process and fine tune them.

Finally, the analysis in this study offer some first steps to arrive at a measure for the amount of convergence that takes place during a collaborative effort. By comparing the results from the 'generate' activity to the results of a 'converge' activity that both relate to the same set of contributions, we can compare to what extent the final outcomes have been condensed and overlap has been removed. As can be seen in tables 2 and 3, comparing these indicators can yield insight into more than just the results of the separate activities. It can also shed light on the extent to which previous activities were exhaustive or if enough resources (e.g. time) were available to complete it.

This study paves the way to using 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.

7. Conclusion

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. Current literature, however, does not provide a collaborative process which practitioners can use to develop a plan unique to their needs. 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, 4) the recovery from the incident, and 5) a follow-up plan to analyze the incident and modify the IRP.

Our results suggest that the concept of a collaborative IRP creating process worked. We received positive responses from the participants in terms of satisfaction with the process, satisfaction with the outcome, and group productivity. These findings are significant in light of the fact that this was an exploratory study with limited time resources to adequately test the process to a successful conclusion.

One limitation was the subjects that were used in each of the three studies. The first pilot study was done with 17 students enrolled in an undergraduate level information security course while the second one was done using ten students enrolled in a graduate level information security course. The final group of eight subjects was done using a combination of computer professionals and information systems security group of the faculty at a university. This resulted in a significant difference in the expertise and experience of these three groups. Although this gave us a somewhat broad view of the issues and modify the process to better fit the experience level of the participants, we did lose a certain level of continuity between groups.

A major factor that inhibited the arrival at an adequate conclusion to the process was the available time. Due to the time constraints involving the availability of the subjects, the process had to be completed in less than 90 minutes. Although a large number of ideas were generated, discussed, and evaluated in this time frame, it did not allow enough time to actually develop a comprehensive plan. This led to a certain level of frustration on the part of some of the participants in that an adequate consensus of opinion was never attained nor issues resolved.

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. There is a need to determine which thinkLets and in which order would be the most effective and efficient use of time and resources. As has been shown, the three cases resulted in modification and improvement. Second, the work of using CE to develop a complete and comprehensive security process that includes such things as vulnerability assessment and business continuity planning would be another big step in expanding this research.

To conclude, we hope that the process design presented in this paper ignites a stream of research that needs to be conducted in the enterprise security arena to

come up with an all-encompassing collaborative process that will cater to all types of security planning procedures.

References

[1] Briggs, R. O., Vreede, G. J. de, Nunamaker, J. F. Jr. (2003). Collaboration Engineering With ThinkLets to Pursue Sustained Success with Group Support Systems. *Journal of Management Information Systems*, 19, 4, 31-63.

[2] Briggs, R. O., Kolfschoten, G. L., Vreede, G. J. de, Dean, D. L. (2006, August). Defining Key Concepts for Collaboration Engineering. *Proceedings of 12th Americas Conference on Information Systems (AMCIS)*, Mexico.

[3] Briggs, R.O., Reinig, B., Vreede, G.J. de. (2006). Meeting Satisfaction for Technology Supported Groups: An Empirical Validation of a Goal-Attainment Model, *Small Group Research*, (in press).

[4] Briggs, R.O., Vreede, G.J. De, Reinig, B.A. (2003). A Theory and Measurement of Meeting Satisfaction, *Proceedings of the 36th Hawaiian International Conference on System Sciences,* Los Alamitos: IEEE Computer Society Press.

[5] Grinsven, J. van and Vreede, G. J. de (2002), Design Guidelines for Risk Management in the Distributed Software Development Process, Pro*ceedings of the International Design Conference*, Dubrovnik, May 14-17.

[6] Kolfschoten, G. L., Vreede, G. J. de, Chakrapani, A., and Koneri, P. (2006), The Collaboration Engineering Approach for Designing Collaboration Processes, *Proceedings of the First HICSS Symposium on Case and Field Studies of Collaboration*, Poipu, Kauai, Hawaii.

[7] Koneri, P. G., Vreede, G. J. de, Dean, D. L., Fruhling, A. L. and Wolcott, P. "The Design and Field Evaluation of a Repeatable Collaborative Software Code Inspection Process," In *Proceedings of CRIWG 2005*, LNCS3706, Fuks, H., Lukosch, S. and Salgado, A.C. (Eds.), Porto de Galinhas, Pernambuco, Brazil, 2005, pp. 325-40.

[8] Poindexter, D., & St. Laurent, N. (2000, May 19). Incident Handling at BMDO (IWS – The Information Warfare Site No. 0008 Ver. 1), Retrieved May 4, 2006 from: http://www.iwar.org.uk/comsec/resources/fasp/BMDOIncHandling.htm.

[9] Vreede, G. J. de, Fruhling, A., and Chakrapani, A. (2005) "A Repeatable Collaboration Process for Usability Testing,", p. 46, *Proceedings of the 38th Annual Hawaii International Conference on System Sciences (HICSS'05)*.

[10] Vreede, G. J. de., & Briggs, R.O. (2005). Collaboration Engineering: Designing repeatable processes for high-value collaborative tasks. *Hawaii International Conference on Systems Science*, Los Alamitos: IEEE Computer Society Press.

[11] Wack, J.P. "Establishing a Computer Security Incident Response Capability." US National Institute of Standards and Technology. Gaithersburg, Md. NIST Special Publication 800-3. November 1991.

[12] Zuber-Skerritt, O. (1991). Action research for change and development. Gower Publishing, Aldershot.

9. Appendix: Initial process design

Table 5. Initial Process Design

Steps	Deliverables	Patterns	ThinkLets
1. Agree on taxonomy	Consensus on the taxonomy		TurnTaker
2. Get input on each incident: Symptoms, COA, Leaders, Recording	Items in each of the categories	Divergence	LeafHopper
3. Clean up the categories	Non-redundant incident ideas	Convergence	BucketBriefing, Concentration
4. Reach consensus on items entered	An agreed upon list of items	Evaluate, Consensus	StrawPoll, Crowbar
5. Assign severity levels for incident type	Agreed upon severity levels	Vote, Consensus	PopcornSort, StrawPoll, CrowBar
6. Get evaluation on design	Evaluation from students	Measurement tool	