5. Davis, A. J., Kamal, M., Schoonover, T. V., Nabukenya, J., Pietron, L.R., and Vreede, G.J. de (2008) Incident Response Planning using Collaboration Engineering Process Developme...

Article · January 2008

CITATIONS
0

READS
151

6 authors, including:

Josephine Nabukenya
Makerere University
46 PUBLICATIONS **252** CITATIONS

SEE PROFILE

Gert-Jan de Vreede
University of South Florida
377 PUBLICATIONS **7,916** CITATIONS

SEE PROFILE

JISSec 4(3) 2008

Journal of Information System Security

www.jissec.org

Incident Response Planning Using Collaboration Engineering Process Development and Validation

Alanah J. Davis

Mehruz Kamal

Terrance V. Schoonover

Leah R. Pietron

The Institute for Collaboration Science
University of Nebraska at Omaha

Josephine Nabukenya

Institute for Computing and Information Sciences
Radboud University Nijmegen

Gert-Jan de Vreede

The Institute for Collaboration Science
University of Nebraska at Omaha
Delft University of Technology, the Netherlands

Abstract

Many organizations have plans for incident response strategies as

[1] An initial version of this research was presented at the Inaugural Workshop on Information Security and Assurance (WISA): Special Interest Group on Information System Security (SIGSEC) Workshop 2006, Milwaukee, Wisconsin, December 10.

part of their contingency planning process. 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 & St. Laurent, 2000). In a nutshell, IRP involves risk reduction and mitigation and focuses on immediate response. Furthermore, Microsoft suggests that "having a detailed, well-rehearsed, and flexible incident response plan ensures that any exploit that occurs can be handled in an orderly, effective manner that minimizes the impact to systems" (Soper, 2003, p. 34).

Increasingly, new security incidents are emerging and the importance of information security policies and guidelines or recommendations is grow-

ing (Dhillon, Backhouse, & Masurkar, 2005). Despite organizations' efforts to respond to these 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; Sausner, 2007) and should provide guidance to mitigate the violations of information security policies across the globe, not just at the local level (Dhillon et al., 2005). An IRP is thus 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. The value of our research concerns addressing the challenge of producing a comprehensive IRP in a short time-frame with many stakeholders. The contributions of this paper are threefold. First, we present a facilitated collaborative process for incident response planning through the use of a collaboration technology, specifically a group support systems (GSS). Second, the process design has been applied in three iterative situations and seen to produce the desired results. Finally, our research lays the foundation for future research in other areas of enterprise security planning (e.g. contingency planning, disaster recovery, etc.).

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 recovery, business impact analysis, 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. The next section gives a background of IRP. The description of our research approach in terms of design and research methods follows in the next section. Then the results from the three iterations are discussed, and the paper ends with a discussion, implications for research and practice and a conclusion with future research directions.

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, Miksell, Nainis, & James,

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 incident response plan (IRP). As mentioned above, this research deals specifically with the IRP.

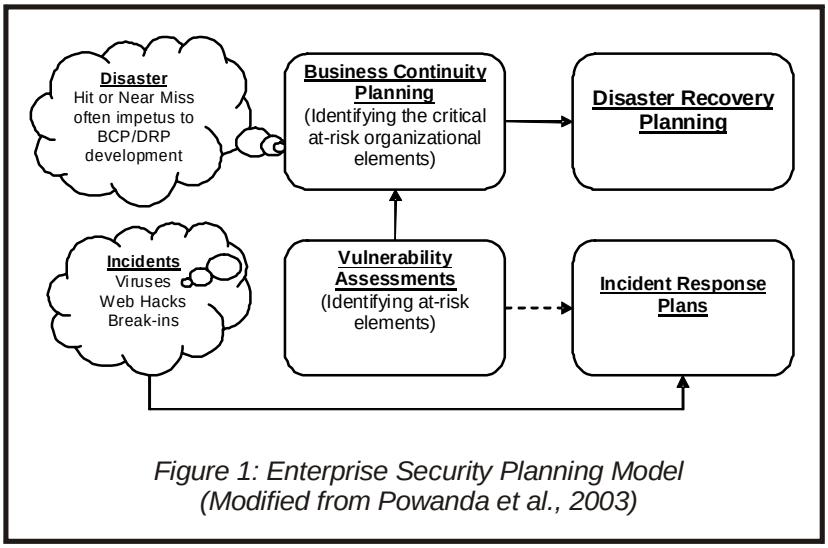


Figure 1: Enterprise Security Planning Model (Modified from Powanda et al., 2003)

IRP covers 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. An example of an IRP process is the Cyber Incident Response Plan (Swanson et al., 2002). This process, depicted in Figure 2, establishes procedures to address cyber attacks against an organization's IT system(s). These procedures are designed to enable security personnel to identify, mitigate, and recover from malicious computer incidents, such as unauthorized access to a system or data, denial of service, or unauthorized changes to system hardware, software, or data (e.g., malicious logic, such as a virus, worm, or Trojan horse).

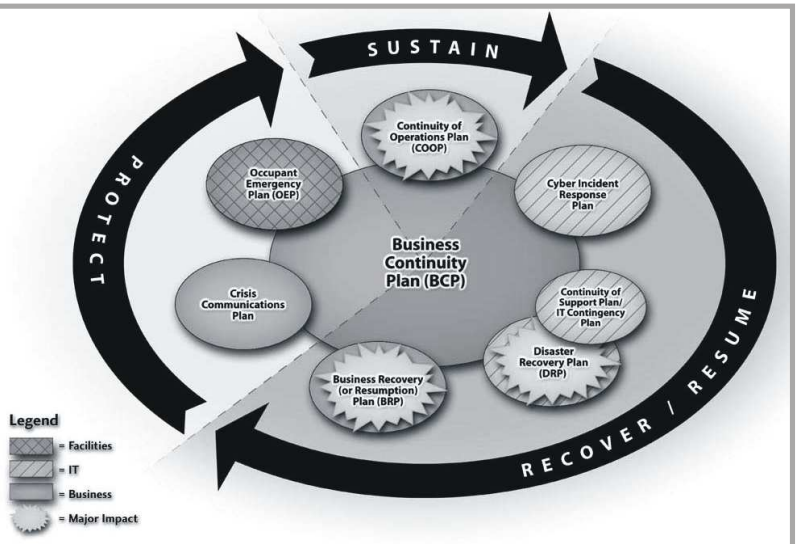


Figure 2: IRP Example: The Cyber Incident Response Plan (Excerpted from Swanson et al., 2002)

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. Furthermore, 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 3.

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).

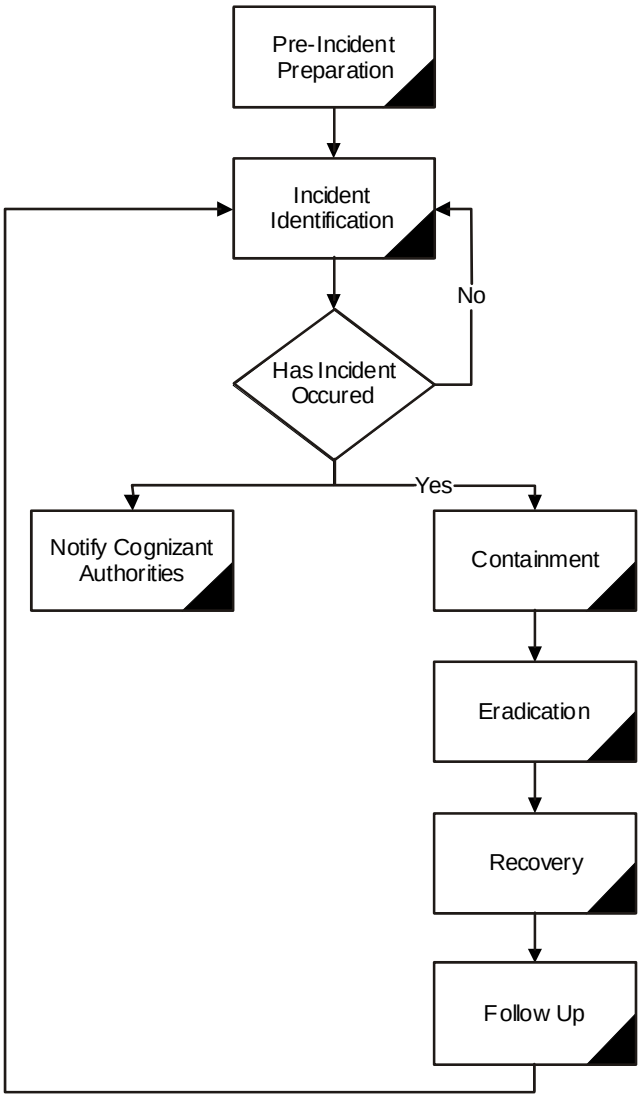


Figure 3: Procedures for Responding to Computer Incidents (Modified from "Computer incident response guidebook," 1996)

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.

Recently, the area of IRP has received increasing attention from researchers. For example, a recent 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, p. 136) 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." 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).

Notwithstanding current advances in the research on IRP, to our knowledge, there has not been any research on the collaborative aspects of creating an IRP. Collaboration is important in establishing an IRP for a number of reasons. Most importantly, an IRP is usually developed in a team or with a group of experts (Foix, 2004; Sausner, 2007); it should therefore be of value to the stakeholders involved to have access to an efficient collaborative creation process. Therefore, this research may be a valuable contribution to the field. The next section will discuss the research approach that we followed to create and evaluate a collaborative IRP creation process.

Research Approach

Our research approach consists of two parts. First, it followed a design method, Collaboration Engineering (CE), to create a repeatable collaborative process. Second, it applied action research principles to evaluate the collaborative process design and improve it. Both parts of the research approach are discussed below.

Design Method: Collaboration Engineering

The choice for developing a collaborative process design for IRP using a 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, de Vreede, & 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, de Vreede, & Nunamaker Jr., 2003), and 3) designing a repeatable process (in this case a repeatable IRP process) has the possibility of creating intellectual capital for organizations (de Vreede & 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 et al., 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, de Vreede, Chakrapani, & 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 et al., 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. 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: Action Research

The development and evaluation of our collaboration process took place in three iterations. These iterations were executed by following an action research approach. As we considered the object of design in our study, a repeatable collaboration process, to be too complex to be tested in a lab setting, we felt that a field study method was the most appropriate. Furthermore, we considered action research to be the most suitable field research method to accomplish our research goal. Action research allows for the actual design of an intervention in addition to studying the application of the intervention in practice (Baskerville, 1999). Other field methods such as case studies, ethnography, or grounded theory studies do not include the design perspective (Myers, 2004). Further, action research has been successfully used in other similar studies (de Vreede, Fruhling, & Chakrapani, 2005; Koneri, de Vreede, Dean, Fruhling, & Wolcott, 2005).

In our study, we followed the action research process proposed in (Zuber-Skerritt, 1991). This process states that an action research study consists of four phases that can be carried out over several iterations (three in

our study): 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 iteration, the process of reflection took place in which we would evaluate what did and did not work in terms of the process.

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

- *Iteration 1*. Student Lab Computer Incident Response Plan with 17 students enrolled in an undergraduate level information security course.
- *Iteration 2*. Student Lab Computer Incident Response Plan with ten students enrolled in a graduate level information security course.
- *Iteration 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 iteration the group used a GSS as a collaborative platform to produce a 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:

Sources for Data Collection	
Direct Observation	Using a pre-defined observation instrument researchers made notes of: - critical incidents - questions from participants relating to the work shop 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 iterations 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 iteration, continuous improvement of the design was done. The analysis 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 iterations (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.
- . 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 iteration to iteration. 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 iterations 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.

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**	**0**
	1.92%	**0.63%**	**0.0%**
Contributions per participant	**0.18**	**0.10**	**0**

Table 2: Contributions from brainstorming activity

Convergence	**1**	**2**	**3**
Total	**134**	**139**	**182**
Contributions per stakeholder	**7.88**	**13.9**	**22.75**
Unique	**132** **98.51%**	**136** **97.84%**	**182** **100%**
Contributions per participant	**7.76**	**13.6**	**22.75**
Off-task	**10** **7.5%**	**0** **0.0%**	**0** **0.0%**
Contributions per participant	**0.59**	**0**	**0**

Table 3: Contributions from clean-up activity

Application Results

The final output from the teams in each iteration resulted in a useable IRP. Figure 4 presents the course of action in response to virus and worm incidents that was delivered in Iteration 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 4: Iteration 3 Course of Action deliverable for virus and worms

Additionally, the General Meeting Assessment Survey questionnaire (Briggs, Reinig, & de Vreede, 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 et al., 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.

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

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 brain storming 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.

Discussion

As has been discussed earlier, new security incidents are emerging and the importance of information security policies and guidelines or recommendations is growing (Dhillon et al., 2005). Specifically, having a successful contingency plan in place is paramount to the minimization of damage from an information security incident (Stacey, 2005). Organizations need to have an IRP in place to support contingency planning, 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. There has, however, been little research on the development process 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 (Foix, 2004; Sausner, 2007). 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 evaluate a collaborative process for the creation on an IRP that would be both workable and repeatable. To this end, we refined a collaboration process design in three iterations using feedback from observations, surveys, and interviews. The designed 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. The results of the three iterations 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.

According to Sausner (2007) "one size doesn't fit all" when it comes to dealing with incidents and having a response plan and team in place. 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.

This research makes several contributions to IRP research and practice. 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.

Finally, a key implication 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.

Conclusion

As outlined above, the contributions of this paper are threefold. First, we present a facilitated collaborative process for incident response planning through the use of collaboration technology. Second we successfully applied that process in three iterations. Third, our research lays the foundation for future research in other areas of collaborative enterprise security planning (e.g. contingency planning, disaster recovery, etc.) with our process design. This is to say that we have developed an approach (i.e. process) that has worked for a part of enterprise security planning (i.e. IRP). Yet, we expect that similar types of CE processes will work for other areas.

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 and 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. Finally, we are hopeful of expanding this research to 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.

Acknowledgments

We are thankful to the reviewers for their suggestions and to the editor for his constructive guidance.

References

Baskerville, R. L. (1999). Investigating information systems with action research. Communications of the AIS, 2(19), 1-32.

Briggs, R. O., de Vreede, G.-J., & Nunamaker Jr., J. F. (2003). Collaboration engineering with thinkLets to pursue sustained success with group support systems. Journal of Management Information Systems, 19(4), 31-64.

Briggs, R. O., Kolfschoten, G. L., de Vreede, G.-J., & Dean, D. L. (2006, August 4-6). Defining key concepts for collaboration engineering. Paper presented at the 12th Americas Conference on Information Systems (AMCIS-12), Acapulco, Mexico

Briggs, R. O., Reinig, B. A., & de Vreede, G.-J. (2006). Meeting satisfaction for technology-supported groups: An empirical validation of a goal-attainment model Small Group Research, 37(6), 585-611.

Computer incident response guidebook. (1996). Information Systems Security (INFOSEC) Program Guidelines Module 19 Retrieved October 19, 2006, from http://www.marcorsyscom.usmc.mil/sites/ia/references/don/NAVSO%20P5239-19%20CIRT%20Guide.pdf

de Vreede, G.-J., & Briggs, R. O. (2005). Collaboration engineering: Designing repeatable processes for high-value collaborative tasks. Paper presented at the 38th Annual Hawaii International Conference on Systems Science, Los Alamitos.

de Vreede, G.-J., Fruhling, A., & Chakrapani, A. (2005). A repeatable collaboration process for usability testing. Paper presented at the 38th Hawaii International Conference on System Sciences.

Dhillon, G., Backhouse, J., & Masurkar, V. (2005). Meeting the Information System Security Challenge. Journal of Information Systems Security, 1(1), 1-6.

Foix, R. (2004). Expanding responsibility for incident response. Computerworld, 38, 28.

Kolfschoten, G. L., de Vreede, G.-J., Chakrapani, A., & Koneri, P. (2006, January). The collaboration engineering approach for designing collaboration processes. Paper presented at the First HICSS Symposium on Case and Field Studies of Collaboration, Poipu, Kauai, Hawaii.

Koneri, P. G., de Vreede, G.-J., Dean, D. L., Fruhling, A. L., & Wolcott, P. (2005). The design and field evaluation of a repeatable collaborative software code inspection process Paper presented at the CRIWG, Porto de Galinhas, Pernambuco, Brazil.

Myers, M. D. (2004). Qualitative research in information systems. ISWorld Net Retrieved September, 2007, from http://www.qual.auckland.ac.nz/

Poindexter, D., & St. Laurent, N. (2000). Incident handling at BMDO. The Information Warfare Site (IWS) Retrieved October 19, 2006, from http://www.iwar.org.uk/comsec/resources/fasp/BMDOIncHandling.htm

Polstra, R. M. (2005). Student papers: A case study on how to manage the theft of information. Paper presented at the 2nd Annual Conference on Information Security Curriculum Development (InfoSecCD).

Powanda, E. J., Miksell, S., Nainis, W. S., & James, H. M. (2003). Guidebook for maintaining a secure operating environment. Information Technology Support Center (ITS) Retrieved October 19, 2006, from http://216.51.95.219/PDF/SC03.pdf

Rollason-Reese, R. L. (2003). Incident handling: An orderly response to unexpected events. Paper presented at the 31st Annual ACM SIGUCCS Conference on User Services.

Sausner, R. (2007). There's No Substitute For Good Preparation. Bank Technology News, 20, 32.

Soper, T. (2003). Incident response: Managing security at microsoft: Microsoft Technical White Paper.

Stacey, T. R. (2005). Best practice in contingency planning or contingency planning program maturity. In H. F. Tipton & M. Krause (Eds.), Information Security Management Handbook: CRC Press LLC.

Swanson, M., Wohl, A., Pope, L., Grance, T., Hash, J., & Thomas, R. (2002). Contingency Planning Guide for Information Technology Systems. Washington: National Institute of Standards and Technology

Wack, J. P. (1991). Establishing a computer security incident response capability. Gaithersburg, Md: US National Institute of Standards and Technology.

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

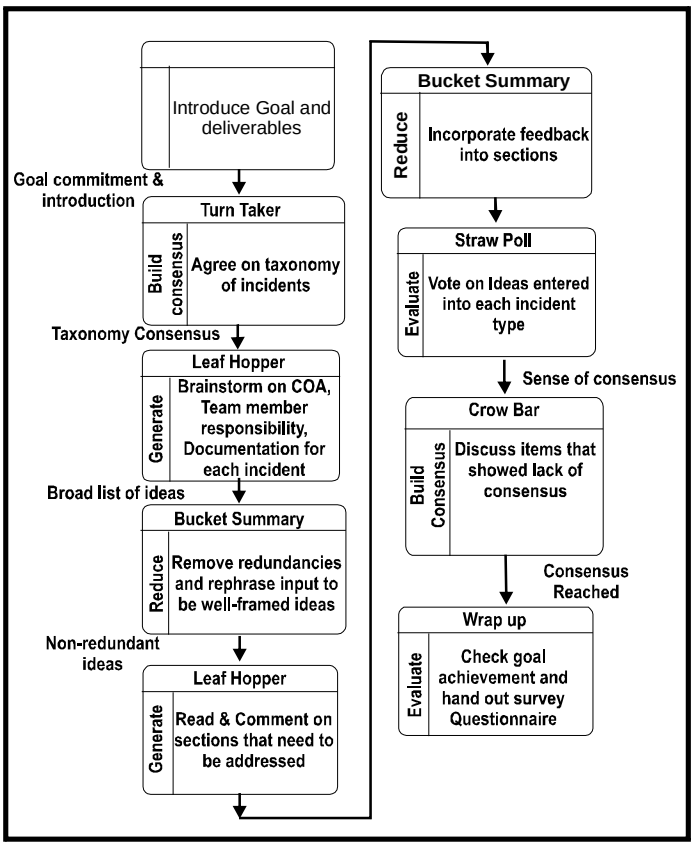
APPENDICES

Appendix 1: 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	Bucket Summary
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	Leaf Hopper

Steps	Deliverables	Patterns	ThinkLet
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	Bucket Summary
6. Reach consensus on the items entered in the categories.	A final agreed upon list of ideas for each type of incident	Vote Consensus	Straw Poll Crow Bar
7. Wrap-up			

Appendix 2: Facilitated IRP Process Flow Chart



Author Biographies

Alanah Davis is a PhD student at the College of Information Science and Technology at the University of Nebraska at Omaha. She holds a master's degree in E-Commerce from Creighton University and a bachelor's degree in both Computer Information Systems and Marketing from Simpson College. Her research interests include collaboration and computer supported group practices in virtual teams and group support systems. Secondary streams of study include e-commerce and interface design. Her work has been presented at conferences such as AMCIS, HICSS, and MWAIS.

Mehruz Kamal is currently a doctoral student at the University of Nebraska, Omaha. Her research areas of interest include but not limited to Collaboration Processes & Technologies, Information Technology for Development, Knowledge Networking, Information Assurance, & Aspect-oriented programming. She has published and presented her research work at workshops and conferences in the area of Information Systems. She holds a Masters and a Bachelors of Science degree in Computer Science from Illinois Institute of Technology. She also possesses work experience in the software industry as a Software Engineer for Motorola Inc., in Arlington Heights, Illinois.

Terry Schoonover is currently a doctoral student at the University of Nebraska at Omaha. He holds a Master of Arts in Management Information Systems and a Bachelor of Science in Business Administration both from the University of Nebraska at Lincoln. His areas of interest focus toward the psychological side of the computer-human interface. These include information systems development, project management, computer-supported collaborative work, and virtual team collaboration. Terry is also currently the Managing Editor of *e-Service Journal.*

Josephine Nabukenya is a PhD student at the Institute of Computing and Information Sciences, Radboud University Nijmegen, The Netherlands. She is also an Assistant Lecturer and Researcher in the Department of Information Systems, Faculty of Computing and Information Technology, Makerere University, Kampala, Uganda. Her educational and professional training is in both Information and Computer Science. Her research focuses on issues related to facilitating organizational change by adoption and utilization of Information & Communication Technology (ICT) within different socio-economic contexts; Facilitation of Group meetings; Collaboration Engineering; Analysis, Design and modeling of Information and Systems flows.

Dr. Leah R. Pietron, Associate Professor of Information Systems, holds a PhD and MS degree from the University of North Dakota; a MBA from Northwest Missouri State University, and BS from Mayville State College. In addition, she has done post-doctoral work at the University of Minnesota and Indiana University. Dr. Pietron's work experience include consulting projects

on security policy, security assessments, Sarbanes-Oxley, and ISO 17799 accreditation. Her publications and presentations include information systems development pedagogy, vulnerability assessment methodology, collaboration science, and information assurance distance education.

Dr. Gert-Jan de Vreede is Kayser Distinguished Professor at the Department of Information Systems & Quantitative Analysis at the University of Nebraska at Omaha where he is Director of the Institute for Collaboration Science. His research focuses on Collaboration Engineering, field applications of e-collaboration technologies, and the diffusion of collaboration technology. His articles have appeared in journals such as *Journal of Management Information Systems, Communications of the ACM, Small Group Research, DataBase, Group Decision and Negotiation, Journal of Creativity and Innovation Management, International Journal of Technology and Management, Simulation & Gaming, Simulation, and Journal of Simulation Practice and Theory.*