Initial Steps for IT Incident Visualization: Understanding Leadership Needs, Design and Evaluation

Mark F. Tannian
St. John’s University
tannianm@stjohns.edu

Abstract

In today’s technology dependent world, business leaders within organizations must address information technology (IT) incident response needs. Yet, piecemeal and inadequate incident response tools frequently stymie their engagement. This paper discusses a user-centered approach undertaken to design, develop and evaluate an initial leader-centric IT incident response visualization that would facilitate effective and timely self-directed awareness. Two distinct groups of IT professionals were enlisted in this study. The methodology resulted in an initial development and evaluation of a visualization prototype. The paper introduces management of declared IT incidents as a viable problem domain for visualization. Second, the paper presents the types of information sources for effective IT incident response. Lastly, the paper proposes that leaders would welcome a visualization mechanism that facilitates their ability to observe, understand, synthesize and to adjust real-time actions based on their comprehension.

1. Introduction

IT incidents can be significant events for an organization and to their customers as seen in recent security incidents [1], and operational incidents [2]. The incidents referenced are only two of the recently publicized events, but it is clear that complex systems are prone to operational and security problems. This complexity is in part related to interdependencies and technical sophistication, and these factors will drive the need to involve more specialists and decision-makers. With IT operation paradigms shifting towards adoption of cloud computing [3], the resulting inter-organizational interactions will increase incident handling challenges. A common cohesive understanding of incidents, their impact and the efforts to resolve them will be even more challenging to achieve without tools that facilitate awareness, communication and coordination.

A study was conducted to determine if a visualization system has the potential to provide timely and interactive situational awareness accommodating leaders. In an effort to develop a visualization system that improved leaders’ awareness of the business impact of IT incidents, a user-centered design project was conducted with cooperation from IT professionals. This effort began with the basic premise that current IT incident management tools underserve leaders, and that visualization was a means to address their needs. A field-study group comprised of a set of IT professionals was iteratively contacted to inform and provide feedback to understandings and designs developed from previous interactions with them.

Thousands of IT incidents might occur within a mid-sized enterprise, but not all merit active leadership involvement. The class of IT incidents considered for this research was defined as: an event that negatively affects the integrity, confidentiality and/or availability of information and information systems. These events have sufficient impact or risk that merits the collaboration of leadership personnel beyond the responding workgroup.

This paper offers several contributions to the discussion of visualization. The first is to introduce management of declared IT incidents as a viable problem domain for visualization. Second, the paper presents the types of information sources for effective IT incident response. Lastly, leaders welcome a visualization mechanism that facilitates their ability to observe, understand, synthesize and to adjust efforts based on their understandings.

This paper provides the problem domain context, explores related work, describes the visualization, and presents the evaluation and discussion of the visualization study.

2. Problem Domain

In order to explore current practices and needs, a field study was conducted involving seven
professionals with leadership roles over a period that spanned 32 months, 85 sessions and over 113 hours of recorded interviews. Within that range of involvement, these professionals participated in 23 sessions and over 28 hours contributing to a task analysis effort that was based significantly on [4, 5]. The following business sectors were represented: financial services, insurance and state government. The average level of IT experience among the seven was 20.9 years. Five of the professionals held leadership positions and two were senior technical staff. From an incident handling perspective, of the seven, there was: one business leader, two IT leaders and four incident coordinators. One functioned as an incident coordinator primarily in the public-safety space, which helped broaden the design input by providing insights from an alternative logistically challenging, time-critical and diverse incident field. The public-safety coordinator had limited influence on the IT sensitive dimensions of the user-centered design process.

2.1 Leadership Roles

Five IT incident response roles were identified. Four roles were leadership positions and the remaining role, “Response Team Member,” represented the staff responsible for executing tasks that lead to IT incident closure. The first leadership role, “Incident Coordinator,” in many ways the central figure, was responsible for timely incident investigation and restoration of normal operations of the affected systems and data. The second, “IT Leader,” had a varied set of responsibilities, but was primarily responsible for the availability and operational integrity of one or more of the systems affected by the incident. Next, “Business Leader,” functioned as the “customer” of the affected services. The Business Leader role was responsible for being aware of and establishing an understanding of the incident’s impact and ongoing risk on business responsibilities. Business Leaders may initiate protocols within the scope of their resources to minimize the business impact of the incident. The final leadership role was “Stakeholder.” The Stakeholder had few responsibilities with actual response efforts, but had a need to be aware of the incident. Interdependencies of business processes, systems and personnel within an organization require a Stakeholder to monitor an incident’s progress, because the incident’s scope may encroach on their operational responsibilities. The Stakeholder may offer or be called upon to provide resources to help expedite the incident’s closure. One field study participant mentioned that a Stakeholder might be a regulator who is present as a result of the organization undergoing active regulatory scrutiny at the time of the incident.

Although the roles appear to have definition, the assignment to these roles is not predetermined. An incident’s nature dictates personnel assignment. There are numerous dimensions to an incident, but the most dominant with respect to personnel assignment are the affected systems, business processes and business units. The specific role assigned to a person is determined by their knowledge, training and leadership responsibilities within the organization.

The population of assigned incident-handling personnel and their relevant roles may change over the lifecycle of an incident. An incident is a dynamic event that may require additional or alternative skill sets and authority to address it effectively as it progresses. Reductions in personnel and effort priority occur as the incident’s perceived urgency wanes.

2.2 Challenges

Currently, tools that provide situational awareness are primarily geared for technical staff. The business context of events needed by leaders originates from interpretations performed by senior technical staff and the Incident Coordinator as they digest incoming incident details and prepare to communicate with leaders. Many leaders receive their situational awareness through meetings, conference calls and web portals that rely heavily on manual efforts to populate with relevant content. IT Leaders may relocate into operational centers at the risk of disturbing efforts as they try to maintain a more timely awareness.

An IT incident’s impact is magnified by the disruptions to scheduled projects, efforts and operations that lose resources to the response. In order to minimize this secondary impact, leaders cannot typically allow themselves to be consumed by the incident unless its scope or significance relative to assigned responsibilities requires exclusive focus. This resulting multitasking hinders their ability to maintain situational awareness as well as the timeliness of decisions they must make in order for the response to proceed in a timely and cost effective manner.

IT incident metrics remain limited in terms of recognized meaning and method of calculation. Many metrics are subjective and determined without much evidence to make them concrete and reliable. Cost is a recognizable unit of measure, but the methods and mechanisms to compute cost in real-time are limited. Cost is commonly tallied after the incident is closed, thus, making reasonable cost related judgments difficult to perform as the response is underway. Urgency is a subjective measure that has significant influence on resource commitment and timelines, and appears to be computed intuitively based on an inconsistent set of parameters. Business impact or
incident extent, a parameter within urgency computation, is another key metric and is not easily quantified. Systems upstream and downstream from affected systems could either be direct victims of a malicious attack or become victims as a result of a glitch in the ecosystem. Systems requiring updates from affected systems may go stale. Systems delivering information to affected systems may experience overflows or overwriting prior to consumption. These interdependencies today are expressed verbally, referencing institutional knowledge independently accumulated by each responder, which may not be current or complete.

3. Related Work

There is a considerable body of work related to security situation awareness, incident identification and analysis through the use of visualization. There are also a number of commercial systems that monitor network and application operations that have graphical interfaces. Much of this work has been devoted to the needs of technical administrators and security analysts. Erbacher and his colleagues have published a number of efforts related to the needs and approaches to assist analysts address behavior identification and situation awareness within operational contexts [6, 7]. In the most recent of those works, Erbacher writes about work done to facilitate situational awareness among first line managers [8]. In Erbacher’s literature review, he indicates that little has been done to support the decision maker. The leaders within the context of the work presented here are involved with response effort because they have response related decision-making responsibilities. Rasmussen et al. presented NIMBLE (Network Intrusion Management Benefiting from Learned Expertise), a tool designed for use in a Security Operations Center (SOC). Their visualization is an analyst’s tool meant to assist in performing triage on activities that have the potential to become incidents[8]. Unlike the problem domain addressed by Erbacher et al. and Rasmussen et al., the incident in the research reported here has been declared, and an active response is being made to address it.

There is an established body of work related to IT incident response. One of the significant sources is the Software Engineering Institute (SEI) of Carnegie Mellon University. The SEI’s focus has been in support of guiding the creation and operations of Computer Security Incident Response Teams (CSIRTs) and incident management processes (e.g. [9, 10]). Beyond encouraging communication and coordination, this body of literature does not include much in the way of understanding the challenges and responsibilities leadership faces. Cichonski et al., in the National Institute of Standards and Technology (NIST) second revision of Special Publication 800-61: “Computer Security Incident Handling Guide” [11] recommend that pre-planned procedures be established giving the incident handler who follows procedure the authority to execute. Foreseeable or routine incidents can be pre-planned and pre-authorized. What the field study uncovered was the IT incidents of greatest challenge are those that are unanticipated or unforeseeable in these circumstances leadership must take an active role in response in order to satisfy their responsibilities.

Recently, at the Hawaii International Conference On System Sciences (HICSS), in the areas of Public Safety and Emergency Management, visual analytics and visualization have been proposed. If one sets aside the technical and social differences between IT incidents and these topics, there are a number of objectives and challenges in common. Localized and specialized information sharing challenges reported by Jayaraman et al. [12] are similar to challenges leaders face as they attempt to build a composite status picture from available sources. The time sensitive situation awareness objectives being addressed by Nadya et al. [13] and use of animation of social media streams may be relevant for the Incident Coordinator’s situational awareness when incorporating analysis of helpdesk calls. Resource acquisition and tasking were highly preferred features for an IT incident visualization system and were part of the visualization prototype. The resource management objectives mentioned by Arias-Hernandez and Fisher in [14] are fairly similar, but in IT incident response the dominant resource type is labor as opposed to equipment and supplies. There may be opportunities in the future to take advantage of commonalities that exist between IT incident handling and Public Safety and Emergency Management.

4. Visualization

The visualization designed was the result of an iterative process. The selection of IT incident management as a problem domain was identified and prioritized by the professionals in the field study. The field study proceeded with a domain investigation that involved these same professionals. From the investigation, a set of requirements was developed and reviewed with the study participants. Based on their feedback, these requirements were prioritized by the study group using a process based on Analytical Hierarchical Process (AHP), which has been used in past software requirements prioritization efforts[15]. After computing the AHP results, a preference threshold scheme was used to provide guidance as to which requirements should be dropped. The scheme
involved putting requirements in ranked order and aggregating preference values. Those ranked requirements that were within the preference aggregate threshold were strong candidates to be the basis for the design effort.

A paper-based prototype was initially designed to satisfy these requirements. The low fidelity prototype consisted of screens with alternative views and screen navigation flows. The prototype was reviewed with the field study group exploring appropriateness, missing elements and alternative metaphors. From that point, a medium fidelity prototype was developed using Microsoft Expression Blend and C# to build a web-based Silverlight web browser application. The field study group reviewed this application. Another group of professionals was enlisted to perform an evaluation on the prototype.

4.1 Design Requirements

The requirements discussed here were the design requirements used to motivate the low-fidelity prototype that in turn led to the medium-fidelity system. The requirements were developed as a hierarchy in order to facilitate their meaning and prioritization. There were nine top-level requirements and three to five second-level sub-requirements for a total of 37 second-level requirements. The requirements effort was not limited to identifying interactive visualization requirements. The requirements attempted to capture the overall problem domain needs in order to provide a broader context in which the visualization system would exist. Given the space limitations of this paper it is necessary to refer the reader to the original documentation of these requirements for a description of top-level and second-level requirements [16]. The list below provides the top-level requirement labels:

1. Incident Handling Awareness
2. Decision Support
3. Communication Capability
4. Coordination Capability
5. Incident Actions Guide
6. Incident Measures
7. Incident Review & Analysis Tools
8. Incident Handling Documentation
9. Visualization Usability

The high-level requirements show that professionals desired that a system not only facilitate awareness and understanding, but enable command and control. Complex IT incident commonly require multiple workgroups in multiple locations to be coordinated and the responders’ efforts be communicated to leaders not necessarily collocated. Decisions that require input from multiple people can be difficult to coordinate as a real-time interaction due to time zone and location diversity as well as competing obligations. Catastrophic incidents that would receive absolute priority are outliers. Incidents in this study are those that involve collaboration of leaders and staff from multiple workgroups primarily due to the extent of the incident spanning across areas of responsibility.

4.2 Requirements Prioritization

The review process with the study group professionals resulted in several alterations of language and several additional requirements. Professionals within the group did not propose that any of the requirements were without merit. The design effort could not provide equal emphasis or support for all the requirements. The AHP process provided a significant amount of clarity. The conceptual dependencies among requirements prevented a strict interpretation of a preference threshold requirements incorporation approach. For instance, how could a system provide IT incident support without addressing time as a fundamental parameter?

Figure 1 shows a Venn diagram of the second-level requirements arranged by whether they fell within the 70% preference threshold for a role. The field study professionals were asked to rank the requirements from a specific role’s (Incident Coordinator, IT Leader, Business Leader) perspective. Requirements outside of the sets did not receive sufficient preference to be incorporated within 70% preference threshold. An implicit role of “every role” is represented as requirements in bold text. The “every role” was the aggregation of second-level requirement preference ignoring the role context. Requirements encapsulated by a border were those that would manifest visually. The number-letter combination in the labels refer to a requirements description document in which the number represents the high-level requirement category and the letter is a unique label for the second-level requirement within the respective category.

When these requirements preference values are viewed from a perspective of expectation, one can interpret the preference results with greater understanding. Kano Noriaki proposed a product quality model called the “Kano Model” that categorizes requirements or product features in terms of customer satisfaction. The model has three levels: expected, normal and exciting. It is reasonable to interpret the highest preference within the AHP process to be those requirements that are the most interesting or exciting. For more details about how these second-
level requirements fell into these Kano categories, see the original description of this process [16].

By utilizing interpretive viewpoints of AHP preference distribution, the Kano Model and requirement dependencies, a prioritized list of requirements was established. As the specific design and implementation efforts progressed, additional requirements were put aside or reprioritized. More details will follow in the Evaluation section, but in sum the “deployment” context took greater precedence as this design effort transitioned from ideas to software. The operational context of the final system was an academic evaluation as opposed to a fielded product. The time available to the evaluation process was extremely limited, thus making some features less likely to be utilized given the real-time incident management tasks considered most relevant for evaluation.

4.3 Tasks

Tasks in IT incident response can vary based on the specific plan being executed. These response tasks may be mapped into a sequence of user tasks within the context of using the visualization. An initial catalog of usage tasks was developed. This study did not endeavor to catalog the array of response tasks across the array of incidents and industries represented by the study group membership.

The usage task catalog aligned fairly well to the second-level requirements. This was due to the iterative nature of the task analysis and attempts to formulate a concise set of requirements. To borrow a term from Sedlmair et al. these usage tasks were somewhat “fuzzy” [17]. The incident response role of a user influences the frequency a particular task is performed. The following is an abbreviated list to illustrate types of usage tasks:

- Get started (login)
- Achieve general awareness of business
- Achieve updated awareness of incidents
- Perform decision/judgment task
- Acquire response resource

4.4 Data Needs

This study identified some data needs that may not be readily addressed in today’s environments. This is in part due to the lack of systematic collections of relevant information and the lack of formal definition of measures as well as their input sources. It was necessary to fabricate information collections that may not commonly exist in order to conduct the evaluation. The following is a partial list of the data sources necessary for the features identified to be functional:

- Business process health monitoring
- Direct costs that relate to labor, resources, revenue loss, productivity loss, calculable penalties from contracts or regulation
- An integrated catalog of business processes, systems, information collections, personnel and physical location
- Human resources records that include operational status, skills and related proficiency, contact information, management
- Machine readable response plans that include task details like needed skills, objectives, constraints

4.5 Design

One research objective was to evaluate whether professionals would perceive visualization for this problem domain as beneficial. This objective had a significant influence in the visualization design and the platform chosen. The evaluating users were invited to volunteer during the limited time of a normal workday. The original estimate was 60 minutes with twenty minutes devoted to actual interaction with the visualization. User training was limited to a brief introductory presentation and a video that started after logging into the application. Within this concentrated experience, the objective was for evaluators to find meaning, make decisions and consider the broader value of visualization in the IT incident response domain. The implementation had to balance between general domain supports and ensuring that functionality relevant to the scenario was available.
The datasets used during the evaluation were synthetic, and needed to be conceptually reasonable and coherent.

The interface that facilitated the evaluation was chosen as an integral part of the user experience. This resulted in the visual space for visualization system being bordered by the indicators and controls needed to progress through the evaluation exercise. In Figure 2, the evaluation interface is the light blue regions. In order to improve the clarity of the remaining pictures related to the visualization presented in this paper, the evaluation interfaces were cropped out. The platform on which evaluation users performed the evaluation tasks was a Microsoft Windows 7 low-mid grade laptop connected to monitors capable of rendering 1680 x 1050 resolution. The visualization application needed to be self-contained, without networking; so all relevant data was embedded as part of the application package. The lack of networking simplified setup and reduced security concerns of hosting facilities. External mice and keyboards were provided allowing the laptops to be set aside and the users to focus to be on the monitors. Although audio was not used to facilitate analysis or awareness within the visualization, audio was used in the training video embedded within the application. With multiple self-directed evaluations occurring simultaneously, supra-aural headphones with generous cabling were provided as well.

After considering the usage tasks, the datasets, the evaluation constraints, it was determined during the low-fidelity prototype design phase that multiple screens would be needed. The low-fidelity design investigated distinct user experiences for the Incident Coordinator, IT Leader and Business Leader. This was driven by the Functional Relevance and Information Relevance second-level requirements as seen in Figure 1. Anticipating that there would be recruitment challenges for those professionals with Business Leader and Incident Coordinator experience, the medium-fidelity prototype implementation was limited to the IT Leader role. The medium-fidelity implementation had 13 distinct screens, many with multiple views.

The evaluation was designed to be a goal-oriented tour through the system. There was time for only one incident exercise from which evaluating users would be asked to extrapolate based on first impressions and limited use.

A driving consideration in the design was the issue of cognitive fit[18]. There was insufficient data to suggest which tasks could be addressed strictly in graphical form. Juxtaposing graphic and textual elements can become visually unmanageable as the number of dimensions and/or data density increases within a graphical presentation. A conservative approach was taken to develop the first visualization in the problem domain. Tabular views, many of which were interactive, were provided as alternative views or if no established visual metaphors were deemed readily compatible with task objectives and related data. The result was similar to an advanced dashboard. Given the limited time evaluating professionals had to learn and adapt, familiar tabular constructs were anticipated to be necessary.

The Grand Summary screen, as seen in Figure 2, is the first screen of the visualization after logon (evaluation users were requested to click through a disclaimer and watch a training video). This screen presents a business operations view and an incident monitoring view. The Incident Monitoring section provides the user high-level awareness of open incidents. The Incident Monitoring interface is based on a quadrant metaphor on which incident glyphs are positioned based on two contributing sub-measures within incident urgency, namely response execution risk and direct cost risk. As previously mentioned, urgency as an IT incident measure does not currently have a formal means of computation. A method of computation was devised for the purposes of this visualization. The diameter of the glyph is proportional to incident urgency and the incident ID’s label has variable clarity based on relevance to the user. A user only has access to incidents to which they have been assigned. By clicking on the glyph, the user transfers into an incident centric collection of screens. The screen collection in concept is role sensitive, but in practice only the IT Leader role-based collection is available.

The remaining 12 screens are located within three primary categories, which are incident content, response content and institutional context. Each content area has a readily accessible “summary” screen that provides a broad view of the current content area information. Greater detail of constituent data is
The features that allowed a leader to adjust the response effort were placed on screens within the response content category. Details were commonly located on distinct screens that were accessed by navigation controls. Navigation to the detail screens was made explicit as opposed to a “drill-down” behavior. With limited training, unapparent affordances to greater information detail and features would likely be ineffective. The drill-down feature in the Grand Summary to access particular incident centric screens was explicitly mentioned in the training video.

The “Response Plan” interface, shown in Figure 3, within the “Response Summary” screen is based on the activity diagram metaphor. The response plan is the cornerstone of the response-oriented data that is being computed and depicted in various formats. A key challenge with IT incident response today is for all participants to be aware of what the response plan entails and current progress to that plan. Technical responders who work closely together keep each other informed verbally or through helpdesk systems, but leaders tend not to access or interface with the response in the same manner. In complex unanticipated events that are likely to benefit from this visualization, detailed predefined plans are unlikely to exist. During the low-fidelity design effort, plan authoring and editing interfaces were considered, but they were not implemented in software. On-going adjustment to plans was anticipated because the nature of an IT incident can change or understanding improves after initial efforts are completed. The visualization design anticipated that each distinct incident might have a unique response plan. By selecting a Response Plan object a user can see various details related to the selected task.

Timeline and dependency monitoring was a feature that received significant preference for all roles. By understanding current and anticipated resource challenges, leaders can formulate revised resource commitments. After exploring a variety of metaphors, the Gantt chart resonated the most during the low-fidelity prototype design review. This interface is updated continuously. Traditional Gantt parameters such as task start time, task duration, predecessor tasks, critical path and slack are updated as time and response efforts progress. As shown in Figure 4, below each glyph is a progress indicator informed by status collection provided by responders. This modified metaphor draws the leader’s attention to a number of logistical challenges. Not all dependencies within a plan are logical, but are due to resource constraints. These resource dependencies are depicted. An indicator, in the key in the left panel, calls attention to under-provisioned tasks. Simultaneous tasks with a common resource assigned are flagged as well, because that resource cannot realistically address all those tasks within the same timeframe. Resource availability issues are indicated as well. Within a dynamic response effort, original resource assignments may no longer be viable as tasks are delayed or task durations extend beyond expectations. The rotated square glyphs, which are decision tasks, are a common glyph used in this metaphor as well as on the activity diagram. The formal designation of decision tasks was deemed necessary because any formal decision-making performed in these incidents would involve leaders. This distinct symbol assists leaders in locating their upcoming obligations to the response effort. Common IT incidents with limited extent have common procedures, and in some organizations decision authority is delegated to senior technical responders, but for the unusual and cross-organizational nature of the IT incidents of interest the decision burden is on leadership. Task glyphs within the timeline can be selected and details related to that task could be seen in the bottom pane. Placing the details below the graphical presentation avoided obscuring the broader context in which a particular task exists.

Figure 3: Response summary screen with graphical view visible

5. Evaluation

The evaluation process consisted of conducting a number of structured evaluation sessions; at which enlisted IT professionals were asked to evaluate the visualization research. Professionals from the field study were excluded from these sessions. The sessions were designed to minimize inter-session variation of users’ experiences. These events involved bringing equipment to facilities convenient to the evaluating professionals. Due to vehicle capacity restrictions, evaluation facility constraints and overall manageability, an evaluation session accommodated six people. A single researcher facilitated all of the evaluation sessions to further improve inter-session consistency. The event began with an initial paper-
based survey that was followed by an introductory presentation. Following the presentation, all professionals present were asked to logon and work on their own on the provided computer. Prior to starting the first task, a training video of seven minutes in length started immediately after logging in. Twenty minutes was budgeted for hands-on completion, but users could exceed that time limit if needed. Following the hands-on experience, the professionals were given a paper-based survey that elicited feedback on the visualization system. These surveys were the only means of user input formally collected.

Figure 4: Timeline and dependency monitor

Prior to the evaluation sessions, test runs were conducted among available field-study participants. During the test runs the surveys were administered and discussed, the prototype was tested and the introductory presentation was given. Modifications to the surveys, prototype and presentation were made incorporating the input provided.

Recruiting professionals for the evaluation sessions posed a challenge. Distributing the calls for participation and getting professionals to set aside time in their schedules was difficult. The most successful method was to identify advocates within organizations to promote and encourage participation. Six evaluation sessions were held, but qualified professionals attended only four sessions. Eighteen professionals participated, but only seventeen were considered valid. The eighteenth was eliminated due to the participant refusing to answer demographic questions that were needed to measure a participant’s level of experience with IT incident handling.

Evaluating professionals had a median age of 42 with a median of 15 years of IT experience. The median tenure with their current employer was 12.5 years. All but two participants had served in a leadership capacity during an IT incident. Twelve participants had served in the IT Leader role, which was the targeted role. Of the five who had not functioned in the IT Leader role, three had performed the duties of an Incident Coordinator. The participants came from higher education (two), financial services (six), insurance (six) and state government (three). Of the seventeen, eight considered their general incident response responsibilities as “dedicated” and nine considered their responsibilities to be “as needed.” The implication is that eight professionals have a high expectation of being involved in IT incident response.

5.1 Evaluation tasks

Evaluators were assigned six tasks during the hands-on activity. The tasks appeared in the bottom Evaluation Interface panel. No restrictions were placed on their use of the visualization, but instructions suggested several screens that were most relevant to the task at hand. Evaluators expressed their decision by selecting one of several decision options and committing to that decision. Literal task language can be found in the research document [16].

Each subsequent evaluation task took place later in the narrative life of the fabricated incident. Evaluators were told that some decisions they made would influence the condition of the incident. The underlying evaluation state machine followed a paradigm very similar to a children’s “Choose Your Own Adventure” book. The final task was to review a preliminary closure report. This served two purposes. Reporting is a feature expected in enterprise products, and thus this task was a means for the evaluator experience a report that could be populated with information assembled, computed and aggregated by a system central to the response effort. The second purpose was to provide evaluators closure of their own, by allowing them to see how successful they were in managing the incident.

5.2 Evaluation results

The post hands-on survey was designed with four sections, which were: “Evaluation Experience”, “From Your Perspective”, “From Your Firm’s Perspective” and “General Wrap-up.” The Evaluation Experience section was designed to have evaluation participants reflect on the hands-on activity itself. The From Your Perspective section was designed to consider the value of an IT incident visualization system from a personal job responsibilities point of view. The objective of the third section was for the participants to consider the visualization’s value beyond their own needs. The last section was a suggestion field. A thorough discussion of the post hands-on survey can be found in the research document [16].

Within the first section, the participants were asked independent of time constraints, if the tasks were reasonable for the assumed role during the incident.
Fifteen out of seventeen responded that the tasks were reasonable.

In the second section of the survey, there was a question “Would having an IT Incident Visualization System tailored to your firm’s operations help YOU perform YOUR incident handling duties?” The answer options were “No”, “Yes”, “Not Certain”. Among the seventeen responses, nine were “Not Certain”, four were “No” and four were “Yes.” On balance, the collective response to this question was neutral. This could be interpreted to mean that the combination of the quick and intense concept introduction and application was overwhelming, and only after additional opportunities to use the visualization system would they be able to provide a more definitive response. The next question was a multipart question of four yes/no questions. Participants were asked based on their recent experience would an IT incident visualization system be effective to provide them essential facts, present action related options, assist with appraising potential impact across the firm and document past and future actions, outcomes and decisions. Table 1 shows the results (out of seventeen responses) of this question.

<table>
<thead>
<tr>
<th>Effectiveness Area</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provide facts</td>
<td>13</td>
</tr>
<tr>
<td>Present action related options</td>
<td>9</td>
</tr>
<tr>
<td>Assist with appraising impact</td>
<td>10</td>
</tr>
<tr>
<td>Document past and future actions, outcomes and decisions</td>
<td>17</td>
</tr>
</tbody>
</table>

The third section had a question with two parts. The first part asked participants yes/no question whether an IT incident visualization system tailored to their organization would improve IT incident handling decision processes. A response of “No” would be sufficient for the entire question and a response to the five listed advantages within the second part was not requested. Three participants said “No” to the first part and fourteen said “Yes.”

The second part listed five potential advantages and asked participants to indicate the degree of advantages by choosing a value of “Many”, “Some”, “Very Few.” Table 2 presents the advantages and their degree indicated by the fourteen who said “Yes” to the first sub-question.

Within the third section, a different question asked whether a visualization system tailored to the participant’s firm would reduce the average time to closure on IT incidents. Participants had three response choices of: “No”, “Yes”, “Not Certain.” Out of seventeen responses, thirteen answered “Not Certain”, one answered “Yes”, and three indicated “No.” The high degree of uncertainty may be attributable in part to the insufficient time to process what they had learned, the limited range of experiences, lack of a realistic team dynamic within the simulated experience and limited implementation of the functionality within the prototype.

<table>
<thead>
<tr>
<th>Advantage</th>
<th>Many</th>
<th>Some</th>
<th>Very Few</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident Awareness</td>
<td>8</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>Understanding Complexity</td>
<td>4</td>
<td>9</td>
<td>1</td>
</tr>
<tr>
<td>Recognizing Range of Incidents</td>
<td>5</td>
<td>7</td>
<td>2</td>
</tr>
<tr>
<td>Understanding Internal Impacts</td>
<td>9</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>Understanding Outside Impacts</td>
<td>4</td>
<td>6</td>
<td>4</td>
</tr>
</tbody>
</table>

The last question in third section asked if the visualization system were fully integrated within the participant’s firm how would they describe the benefit to their firm. The response choices were “No Benefit”, “Minimal Benefit”, “Good deal of Benefit” and “Exceptional Benefit.” Out of seventeen responses, four responded “Minimal Benefit” and thirteen responded “Good deal of Benefit.” This feedback indicates that despite the limitations of the prototype, participant training and incident experiences, participants thought an IT incident visualization system could be of value among their respective organizations.

6. Discussion

The goal of this research was to introduce and validate an applied visualization concept, and explore IT incident response visualization. The prototype design effort put forward a number of underlying information concepts, visual constructs and a juxtaposition of these elements as a unified body of work for evaluation.

This study went beyond the existing sources of IT incident response information and IT incident measures, and proposed an initial baseline visualization to encourage further research efforts in the IT incident response problem domain. Having this visualization objective and its related value in mind, the gaps among the information sources and incident measures may be steadily addressed in the future. Enterprise management software vendors may likely fill the gaps
because IT portfolio management and other management systems exist in some form today.

When one considers Sedlmair et al. as an assessment criteria of this study, one could evaluate the IT incident response problem domain and this study in particular as premature based on their design study suitability evaluation criteria of task clarity and information location[17]. There is no disagreement that deployment efforts would be premature. Yet, the costs and risks of IT incidents, and in particular security incidents, are sufficient motivation to embark on efforts to further refine task clarity and relocating institutional knowledge from within the minds of personnel to external repositories. Also necessary are additional investigations into refining interaction and visual metaphors appropriate for leaders engaged in IT incident handling. An IT incident visualization system that was ready for deployment would be beneficial to technology-dependent leaders. A new visualization challenge has been set, and further research is recommended.

7. References


