Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2004 Proceedings

Americas Conference on Information Systems (AMCIS)

December 2004

# An Exploratory Investigation of Factors Affecting Computer Security Incident Response Team Performance

Younghwa Lee
*University of Colorado at Boulder*

Sang-Jun Lee
*University of Texas at San Antonio*

# An Exploratory Investigation of Factors Affecting Computer Security Incident Response Team Performance

**Younghwa Lee**
University of Colorado at Boulder
leey@colorado.edu

**Sang Jun Lee**
University of Texas at San Antonio
sjlee@utsa.edu

## ABSTRACT

There has been a huge amount of organizational investment to cope with computer security incidents, but the incidents continue and are expected to increase. Computer security incidents in organizations are primarily dealt with by computer security incident response teams (CSIRT). How the team successfully develops and operates is critical for effective and efficient responses to the incidents. However, no studies have been conducted in that context. This study investigates the factors affecting CSIRT performance based on team performance and crisis management literature through conducting a field study using Delphi method and questionnaire survey. The data are analyzed using Hierarchical Linear Modeling (HLM). We expect the study will provide a useful theoretical framework and practical implications to understand CSIRT performance and thus successfully counteract computer security incidents.

### Keywords

Computer security, computer security incident response teams, crisis management, hierarchical linear modeling

## INTRODUCTION

> "Organizations in which the responsibility for crisis preparation and response rests with crisis management teams will experience greater success outcomes when managing crises than will those organizations in which crisis management responsibility rests with an individual" (Pearson and Clair 1998, p.71).

Computer security incidents (CSI) are more widespread, costly, and commonplace although there has been a huge amount of investment to implement computer security countermeasures According to a survey (CSI/FBI, 2002), 90% of the US organizations surveyed experienced computer security incidents and their volumes are approximately 455 million dollars. Previous studies have found reasons stem from insufficient security systems, inappropriate policy, poor knowledge on computer security, and light punishment. This study, however, explains how computer security incident response teams (CSIRT) successfully develop and operate to cope with the incidents.

CSIRT is a group of people who orchestrate swift and effective responses to computer security incidents by sharing common goals of limiting damage, and reducing recovery time and costs. Considering the fact that successful counteraction of Computer security incidents is highly dependent upon the capability and performance of CSIRT, it is valuable to examine what factors significantly influence CSIRT performance. Based on team performance and crisis management literature, this study develops and empirically tests a research framework of CSIRT performance.

## THEORETICAL FOUNDATIONS

### Team Performance

As organizations require dynamic capability to cope with a rapidly changing business environment, they have structured work around teams rather than individual jobs. The increasing prevalence of teams as the cornerstone of modern American industry is well documented and up to half of the US workforce works in some form of teams. Team refers to a diverse group of people with different backgrounds, abilities, and knowledge levels sharing the same goals and common identity to accomplish a specific task. Compared to an individual, the team is known to provide organizations flexibility, dynamics and synergetic effects, and creative knowledge (Guzzo and Shea, 1992). There has been considerable research investigating factors affecting team performance (e.g. LePine, 2003) and consistently identifying that all individual, team and organizational factors are important to enhance the effectiveness of a team.

### Crisis Management Team

A crisis management team is a group of people within the organization who have been designed to handle a particular crisis. The ability to make correct and appropriate decisions in the midst of a crisis is very important and difficult. Previous studies (e.g. Nunamaker et al., 1989; Pearson and Clair, 1998) have emphasized the value of a team-based approach to cope with crisis. A crisis management team provides a variety of perspectives and skills, facilitates better decision making, accelerates information and resource flow, fosters synergetic contributions, and creates and institutionalizes a positive mind-set under crisis situations.

The key factors for successful crisis management teams have been identified from several studies. For instance, King (2002) investigated five factors that affect crisis management team performance such as prior interactions, team composition, task knowledge, leadership ability, and organization culture, but these were not empirically tested. Weick (1993) examined the factors (i.e. improvisation, virtual role systems, the attitude of wisdom, and norms of respectful interaction) affecting crisis management team performance.

### Crisis Management in the IS field

Compared to numerous crisis management studies in other disciplines, a few studies have been conducted on crisis management in the IS field but no studies have yet been performed to examine CSIRT and its performance context. Housel et al. (1986) proposed a generic set of design guidelines to implement information systems for crisis management. Nunamaker et al. (1989) investigated a set of crisis planning tools to help organizations operate intelligently in crisis situations. Similarly, Hale (1997) developed layered communication architecture for supporting crisis response teams. Finally, Sniezek et al. (2002) examined the influence of crisis management training systems to decision-making performance, called DC-Train to aid decision-making performance.

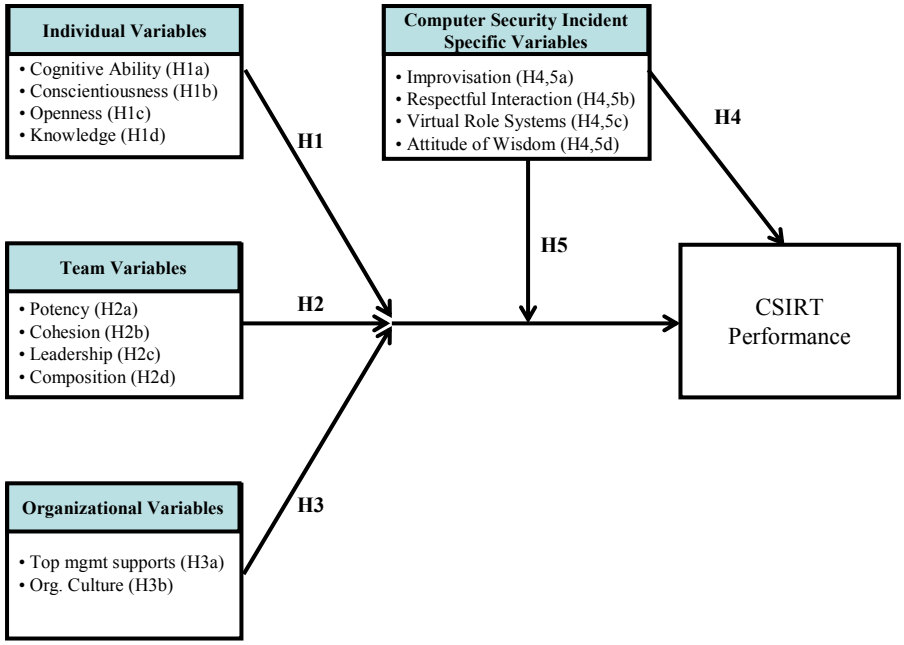


**Figure 1. Research Model**

## HYPOTHESES

Our research framework of CSIRT performance is developed based on team performance and crisis management literature (Figure 1). In this study, security incident is specifically defined as a crisis caused by cyber attacks of malicious outsiders, which prevent normal business operation at least during a couple of hours, resulting in a significant amount of business losses. Team performance refers to the extent to which CSIRT successfully copies with the security incidents.

**Individual Variables:**

*Cognitive ability* is defined as "the capacity to understand complex ideas, learn from experience, reason, problem solve, and adapt" (Devine and Philips 2001, p. 507). Cognitive ability positively relates to task performance, especially in tasks that require high mental representation and manipulation of information obtained from the environment and long-term memory. LePine (2003) found that cognitive ability of team members is especially important while conducting uncertain and unexpected tasks and has a positive relationship with team performance.

*Conscientiousness* refers to "a characteristic that includes feelings of competence, achievement striving, and being self-disciplined" (LePine 2003, p. 29). Studies indicated that highly conscientious individuals have the tendency to set difficult goals for themselves and are more perseverant and committed to those goals. They also have high self-efficacy and expectation and eventually achieve a high level of job performance

*Openness* is defined as "a personality characteristic that reflects imaginativeness, curiosity, originality, and broadmindness" (LePine 2003, p. 29). Open individuals tend to engage in the type of self-monitoring that is necessary for learning in novel situations. They are also positively associated with creativity and receptivity that are crucial to conduct tasks under uncertain, unpredicted, and complex situations.

Team members with prior *knowledge* have a greater understanding of the tasks, are more structured, knowledgeable, and goal-oriented than a team without prior knowledge. Devine and Philips (2001) found that task knowledge becomes more important when the task has a high degree of complexity and a high-level of decision-making among team members.

> **H1**: Team members' cognitive ability (H1a), conscientiousness (H1b), openness (H1c) and knowledge (H1d) are positively related to CSIRT performance.

**Team Variables:**

*Team potency* is defined as "a collective belief by members of a team that the team can be effective across tasks" (Jordan et al. 2002, p. 125). Team potency influences team performance by affecting the extent to which team members apply their resources and effort to the team's tasks (Guzzo and Shea, 1992). Several studies found a positive relationship between team potency and team performance. For example, Hackman (1990) insisted that teams with high potency are more committed and more willing to work hard for the team.

*Team cohesion*, referring to the resultant forces that are acting on the members to stay in a group, is also known to have a critical influence on team performance (Hackman, 1990). Team cohesion is a general indicator of synergistic team interaction or process. When team members have high cohesion, they are willing to assist team members, share feedback, and contribute ideas (Jordan et al., 2002).

The importance of *leadership* for crisis management team performance is also well recognized. King (2002) pointed out that a successfully managed crisis depends upon the team leader's ability to manage the diverse members. The team leader makes organizations return to a state of normalcy using his/her versatile capability such as strong interpersonal skills to inspire and motivate team members, the ability to create symbolic vision and image of competence, trustworthiness, loyalty and confidence.

Past studies also pointed out *heterogeneous teams* perform their tasks better than *homogeneous teams* do (King, 2002). This is because while homogeneous groups are typically less goal and task oriented, which leads to unrealistic and poor team decision-making, heterogeneity promotes the opportunity for diverse opinions and attitudes, freedom of expression, and better decision-making by team members.

> **H2**: Strong CSIRT potency (H2a), cohesion (H2b), leadership (H2c), and heterogeneity (H2d) are positively related to CSIRT performance.

**Organizational Variables:**

Whether a crisis is successfully managed or not is highly dependent on *top management support* for crisis management teams. Pearson and Clair (1998) indicated that a crisis worsens when top management has an ambiguous attitude towards a crisis and the crisis management team. CSIRT needs strong top management support since the team can successfully operate only when top management overtly states his/her support and provides authority to the team.

In the event of a crisis, researchers (e.g. King, 2002) emphasize the importance of *supportive organizational culture* noting that the beliefs and assumptions held by employees within the organization to successfully cope with incidents that affect the

organization's return to normal operation. A crisis worsened when there is lack of common sense and no trust of the crisis management team among employees.

> **H3**: Top management support (H3a) and supportive organizational culture (H3b) to CSIRT are positively related to CSIRT performance.

#### Computer Security Incident-Specific Variables:

*Improvisation* refers to rapid, improvised yet creative and relevant decisions under unexpected, inexperienced and resource constrained situations (Weick, 1993). Studies emphasized the team capability of swift and accurate crisis management decision making and emphasized the training for improvisation capability to make excellent decisions under crisis (e.g. D'Aveni and MacMillan, 1990).

*Respectful interactions* among team members significantly influence the effectiveness of a crisis management team (King 2002). Team members familiar with each other's skills, perspectives, and interpersonal styles might display a freer, more open format of communication under crisis. Gruenfeld et al. (1996) argued that "the greater the number of familiar members in a team, the more open they were to learning from one other, the more they enjoyed working together and the greater their satisfaction with outcomes" (p. 11).

The reconstruction of reality in each team member's head amidst the computer security incidents is called *virtual role systems*. If each team member can simulate other teammates' roles in his/her mind and acknowledge the team leader and facilitate coordination, then s/he literally becomes a team and effectively counteract the incidents (Weick, 1993). Similarly, virtual role systems directly linked to team performance through better quality of communication and quick and high level consensus.

*Attitude of wisdom* refers to acting with knowledge while simultaneously doubting what one knows. That is, extremes must be avoided. Extreme confidence and extreme caution both are closed-minded, which means that neither leads to good judgments. The attitude of wisdom is crucial in making sense of one's environment, particularly in the context of rapid and unpredictable situations. In sum, assuming that CSIRT can successfully fight with computer security incidents if they behave swiftly, with clearly recognizing and respecting each teammate's role and without making extreme decision, we hypothesize that:

> **H4**: Improvisation (H4a), respectful interaction (H4b), virtual role systems (H4c), and attitude of wisdom (H4d) are positively related to CSIRT performance.

Previous team performance studies pointed out that task-specific variables moderate the relationship between antecedents of team performance and team performance (e.g. Hirokawa and Keyton, 1995). In line with the studies, we hypothesize that computer security incidents variables moderate the relationship between individual, team, and organizational variables and team performance.

> **H5**: The relationships in H1, H2, and H3 are moderated by improvisation (H5a), respectful interaction (H5b), virtual role systems (H5c), and attitude of wisdom (H5d).

Finally, this study includes three control variables that have been recognized to affect team performance and examines their effects. They are organization size, and team size and periodical training.

## RESEARCH METHOD

First, we conduct extensive literature reviews on team performance and crisis management. Second, Delphi study with CSIRT or similar team members to find specific computer security incident variables is followed. Third, initial instrument is developed and pretested by experts in related fields (see Table 1). Third, a pilot test is followed to validate the instrument. Finally, a field study using online survey with 132 CSIRTs and their team members (approximately 1,260) is conducted. A high response rate is expected since a prestigious computer security research center sponsoring this project. The data are analyzed using Hierarchical Linear Modeling (HLM 5.0) (Raudenbush and Bryk, 2002) because our study includes both individual and team-level factors. The primary advantage of HLM is that it allows one to simultaneously investigate relationships within a particular hierarchical level as well as relationships between or across hierarchical levels.

| Criteria | Constructs | Items | Instrument Examples |
|---|---|---|---|
| Individual Variable | Openness | 3 | Enjoy learning new solutions to the incidents |
| | Cognitive Ability | 3 | Quickly understand and adapt the incidents |
| | Conscientiousness | 3 | Perseverant until resolving the incidents |
| | Knowledge | 3 | Information of security incidents and sources of solutions and outer experts |
| Organizational Variable | Top Mgmt. Support | 2 | Top managers' resource support to CSIRT |
| | Supportive Org. Culture | 2 | Confidence to overcome the incidents among employees |
| Team Variable | Team Potency | 3 | Confidence to meet any challenges |
| | Team Cohesion | 3 | Closeness among team members |
| | Leadership | 3 | Team leader has strong interpersonal skills |
| | Team Composition | 3 | Diverse ability among team members |
| Security Incident Specific Variable | Improvisation | 3 | Quick consensus under time pressure |
| | Respectful Interaction | 3 | Respectful communication among team members |
| | Attitude of Wisdom | 3 | Make moderate decision making |
| | Virtual Role Systems | 3 | Simulate the teammates' roles in my mind |
| DV | CSIRT Performance | 3 | Time taken to settle down/Team Size |

**Table 1. Examples of Measurement Instruments**

## EXPECTED FINDINGS AND CURRENT STATUS

It is expected to provide a theoretical framework to understand CSIRT performance and empirically validate the framework through an extensive field study. Especially by adopting HLM, we simultaneously examine the effects of both individual-level and team-level factors to CSIRT performance. We also provide useful insights to management on how to create CSIRT and allocate limited resources to manage them.

We are currently in the process of finalizing initial instruments based on extensive literature reviews, and conducting Delphi study. We are confident that we will be able to present study results at the conference.

## REFERENCES (* Full references available upon request)

1. CSI/FBI (2000) Computer Crime and Security Survey, Computer Security Institute.
2. D'Aveni, R. and MacMillan, I. (1990) Crisis and the Content of Managerial Communications: A Study of the Focus of Attention of Top Managers in Surviving and Failing Firms, *Administrative Science Quarterly*, 35, 634-657.
3. Hackman, J.R. (1990) Groups That Work (And Those That Don't), Jossey-Bass, San Francisco, CA.
4. Hale, J.A. (1997) Layered Communication Architecture for the Support of Crisis Response, *Journal of Management Information Systems*, 14, 1, 235-255.
5. Housel, T.J., El Sway, O.A. and Donavan, P.F. (1986) Information Systems for Crisis Management: Lessons from Southern California Edison, *MIS Quarterly*, 10, 4, 389-400.
6. LePine, J.A. (2003) Team Adaptation and Postchange Performance: Effects of Team Composition in Terms of Members' Cognitive Ability and Personality, *Journal of Applied Psychology*, 88, 1, 27-39.
7. King, G. (2002) Crisis Management and Team Effectiveness: A Closer Examination, *Journal of Business Ethics*, 41, 235-249.
8. Nunamaker, J., Weber, E.S. and Chen, M. (1989) Organizational Crisis Management Systems: Planning for Intelligent Action, *Journal of Management Information Systems*, 5, 4, 7-32.
9. Pearson, C.M. and Clair, J.A. (1998) Reframing Crisis Management, *Academy of Management Review*, 23, 1, 59-76.
10. Raudenbush, S.W. and Bryk, A.S. (2002) Hierarchical Linear Models, Sage, Newbury Park.
11. Sniezek, J.A., Wilkins, D.C., Wadlington, P.L. and Baumann, M.R. (2002) Training for Crisis Decision-Making: Psychological Issues and Computer-Based Solutions, *Journal of Management Information Systems*, 18, 4, 147-168.
12. Weick, K.E. (1993) The Collapse of Sensemaking in Organizations: The Mann Gulch Disaster, *Administrative Science Quarterly*, 38, 628-652.