Capabilities and Skill Configurations of Information Security Incident Responders

Mark-David McLaughlin
Bentley University, Cisco Systems
mclaugh_mark@bentley.edu

John D'Arcy
University of Delaware
jdarcy@udel.edu

W. Alec Cram
Bentley University
wcram@bentley.edu

Janis Gogan
Bentley University
jgogan@bentley.edu

Abstract

This paper identifies skill sets that contribute to effective InfoSec incident response. Even though many organizations have staff dedicated to InfoSec incident response teams, there is a lack of consensus as to the skill set each team member needs to effectively perform his/her job, and general and specialized skills that need to be represented in incident response teams (but usually not all held by each team member). Previous guidance was offered based on non-empirical methods. In this study, we used the Repertory Grid (RepGrid) method to elicit lists of incident response skills from industry experts. Skill archetypes were then identified by clustering incident responders who share similar characteristics. The findings extend the Theory of Resource Complements and provide managers with practical guidance regarding the skill sets most critical to the incident response role.

1. Introduction

This paper draws on the resource based view (RBV) and the Theory of Resource Complementarity to closely examining a particular category of resource: employee capabilities. Specifically, this paper clarifies that configurations of general and specialized capabilities are necessary for organizations to develop effective incident response teams. As of early 2016, the Forum of Incident Response and Security Teams' (FIRST) membership included 345 incident response teams in 74 countries [1]. This represents nearly twice as many teams than were listed a decade ago [2] and is only one indication that the incident response role is maturing in modern organizations. Yet, according to a survey conducted in 2015, only 75% of organizational leaders are confident in their response team's ability to identify and respond to InfoSec incidents [3]. Of those leaders that felt their team was up to the challenge, only 40% were confident their teams could handle anything more complex than a simple incident. A majority of managers felt that the crux of the problem was that they were unable to hire qualified job applicants, and that fewer than half of hired candidates were "qualified upon hire" to handle InfoSec issues.

Even though InfoSec incident response teams are becoming a common element in the organizational hierarchy, and even though generally accepted definitions of response team roles and responsibilities exist, there is still no clear guidance on specific skills that individuals need to be successful InfoSec incident responders. Incident response teams encompass many different forms. For example, hardware and software vendors (such as Cisco, Intel, Juniper, and IBM) have created incident response teams to address vulnerabilities in their products; organizations in many other industries have formed incident response teams to address attacks against their information and communication technology (ICT) assets or to respond when they lose customer data; and governments have created response teams to coordinate efforts around remediating vulnerabilities. Some experts observe that as incident response teams have become more common, the role has become much more specialized [4], [5].

Effective incident handling requires an organization to hire InfoSec specialists and this represents a significant investment for organizations [6]. According to the United States Bureau of Labor Statistics, the average salary in 2015 for InfoSec analysts averaged over $90,000 and the demand for information security analysts is expected to grow 18% over the next 20 years [7]. In order to help address this need, this paper helps to define the relevant skills needed for effective InfoSec incident response and identify the various configurations/archetypes of incident response skillsets. Using the lens of the Resource Based View [8], [9] and the Theory of Resource Complementarity [10]–[13], we find evidence that successful incident responders embody unique configurations of complementary capabilities which thus enable individuals to be effective in particular incident response roles.

Specifically, this study addresses the following research questions: In InfoSec response teams:

URI: http://hdl.handle.net/10125/41760
ISBN: 978-0-9981331-0-2

- RQ1: what general and specialist skills or capabilities are needed to effectively respond to incidents?
- RQ2: what is the relative importance of each skill for individuals to be successful in the incident response role?
- RQ3: what capability sets (configurations of complementary skills) are possessed by effective individual incident responders?

Various practitioner and academic studies have attempted to answer the first question, yielding extensive lists of skills that no single individual is likely to possess. However, many of these lists appear to have little empirical foundation and do not explicitly consider whether some skills are more important than others. Addressing this concern, we conducted an exploratory study using the repertory grid (RepGrid) method, which is uniquely suited to identify and evaluate the specific sets of skills that make incident responders effective. Once we elicited the skills critical to the incident response role, we classified and ranked the skills in order to cluster incident responders sharing similar characteristics and develop archetypes of effective InfoSec incident response roles.

The remainder of this paper is organized as follows. First, a review of prior research on resources, capabilities, and skills for information systems professionals is provided. Next, the exploratory study that examined these skillsets is described and the findings are presented. This paper concludes with a discussion of implications and a plan for further study.

2. Literature Review

Given the critical importance of incident response teams and their growing presence in organizations, surprisingly little empirical research examined specific skills or skillsets that InfoSec incident responders should possess. Although various organizations have provided guidance to practitioners, an expectation that an individual would possess all listed skills would be ill conceived. For example, the Software Engineering Institute (SEI) indicates that incident response staff members should have 25 core skills, including both strong technical and interpersonal skills [14], while *SC Magazine* lists 20 core skills that are different from those provided by SEI [15]. Gartner Group's 2016 revision of *Seven Steps to Creating an Effective Computer Security Incident Response Team* lists yet another 11 skills [16] and an empirical study published in *IEEE Security & Privacy* [17] identified another 11 skills that incident responders use when responding to routine and non-routine incidents. Furthermore, some important skills are not yet listed. For example, a recent survey reported that managers overwhelmingly agree that "the largest gap exists in cybersecurity and information security practitioners' ability to understand the business; this is followed by technical skills and communication [3, p. 11]." Yet knowledge of business process and practices is not listed by any of the four organizations referenced, as shown in a combined list of skills from previous lists, shown in Appendix 1.

Another challenge is that incident response tasks are complex, and no manual or textbook offers clear guidance explaining how the job should be performed [18]. The job of incident responder is further conflated by claims that responders may specialize in related areas such as forensics, data mining, reverse engineering, configuration of countermeasures, or penetration testing [5]. One study has recognized the need to distinguish the incident response role (and skills used in that role) by the type of incident (routine or non-routine) [17]. With a lack of commonly accepted, clear guidance, we must turn to empirical research to help identify the skills necessary for incident response teams.

Information Systems (IS) research into the skills needed to be effective in technical fields is not a novel concept, but researchers still struggle to understand this topic. In the 1980's, IS skills studies primarily relied on the Delphi method and surveys of IS managers to generate and rank lists of skills [19]. As the scope of IS work became broader and more varied, this tradition continues today, with researchers focusing on skills needed in specific disciplines, such as IS project management [20], [21] and software development [22], [23]. Other studies addressed IS curricula to develop particular skills in individuals [24], [25].

While many of these studies have helped us understand the skills that can be valuable for IS professionals to have, few provide guidance regarding specific combinations of skill sets that IS professionals effective in their varied roles [20].

Empirical studies identifying skills specific to effective InfoSec incident response have not yet been conducted [26]. Similar to the argument made by Keil et al. [20] examining the skills of IS project managers, a study to identify skills needed by InfoSec incident responders is important because such research will (1) aid organizations in hiring or selecting effective incident responders who demonstrate higher competence in skills viewed to be the most critical for InfoSec incident response activities, (2) help organizations and educators tailor their career development and training programs to further develop response skills among their employees; and (3) help individuals prioritize their own training and development to advance their career.

Like other IS skills, InfoSec incident response skills are strategically important resources and they are most

effective when complementary. An organization is seen as a bundle of human, financial, and other resources [27]. Resources which cannot be easily obtained, are difficult or costly to imitate, and are non-substitutable are the most valuable [8]. IS resources consist of tangible assets (e.g., computers, networks), intangible assets (data, software, specialized knowledge), and capabilities (e.g., an engineer's ability to quickly detect a security violation and formulate a response plan). Assets, individual expertise (capabilities), and the aggregate capabilities of a team can be deployed for temporary strategic advantage [8], [28]. Peteraf [29] explains that expertise in a specialized area such as glass technology provides a strategic advantage. However, just as glass technology could be conceived as the ability to shape, cut, color, layer, strengthen, control breakage, etc. of glass (each of which may take a different set of skills), activities performed in the incident response role might require many or all of the skills included in Appendix 1. At the individual and team levels, some specific attributes – such as integrity, curiosity, or problem solving – may not ensure effective incident response by themselves, yet they have a complementary effect on other abilities (such as risk analysis, knowledge of technical systems, or programming).

Nelson and Winter [30] extensively discussed IS competencies (e.g., IS skills and IS management quality) and IS practices (e.g., culture of IS use). In fact, they devote an entire chapter of their book to the analysis of skills. Relying on the Resource-based View (RBV), they conclude that knowledge is a strategic resource that organizations must invest in. Nelson and Winter further acknowledge that the capabilities of individuals (skills), management quality, and work practices are all resources that have a complementary effect on one another in 'interlocking systems'. The ability of an organization to configure or successfully integrate knowledge-based workers is critical to its success [31], [32]. In other words, when building effective teams, managers must identify individuals with the right combination of skills that complement the combination of skills of others. Still, a recent review concluded that the question of "How, why and when do IS assets, IS capabilities and socio-organizational capabilities affect each other and jointly create internal value?" needs further investigation [33, p. 156].

3. Research Methodology

In this paper, the Repertory Grid (RepGrid) method was used to gain a complete picture of the incident response role and what skills incident responders feel were necessary for their peers to be successful in their role. RepGrid is the methodological extension of Personal Construct Theory (PCT) [34], [35], which takes a social constructivism view in that it focuses on "how human beings create systems of meaning in making sense of and acting in the world [36, p. 145]." PCT claims that every individual continuously creates and re-creates a personalized view of the world that enables him or her to make sense of people, objects and experiences. An individual's view of the world is created by bi-polar constructs which are integrated into unique networks of meaning that enable him/her to interpret current events and anticipate future ones [37]. Individuals are influenced by and share personal construct systems with others and these commonalities are key to interpersonal relationships. Since it is possible to aggregate individual perceptions to understand an organization [38], these common perceptions allow us to apply PCT to organizational studies and, by extension, allow us to aggregate this perception to an industry when the perceptions of individuals working in multiple organizations are examined. In psychology, PCT is a popular reference theory and is cited in almost half of the volumes of the *Annual Review of Psychology* between 1955 and 2005 – largely because of the flexibility of RepGrid as a method that allows for analysis of individuals and groups [39].

In IS studies, the RepGrid technique has provided researchers a means to elicit individual views of work, values, and expectations [40] and RepGrid studies have been extensively adapted to answer a wide variety of research questions. For example, a recent RepGrid study involved interviewing 24 fingerprint technicians to understand their perception of how new technology would alter their work practices [41]. These authors concluded that their modified RepGrid technique "yielded insights into the meaning of fingerprint work that might not have been revealed by more traditional structured interview techniques [41, p. 700]." Another study used RepGrid in interviews of 19 IS project managers to determine the skills necessary for a successful IS project management practice. This study concluded that successful project managers generally fall into one of four skills groups or archetypes [21], determined by clustering individuals with similar skillsets and calculating the percentage of times each skill was mentioned in the cluster.

Beyond IS research, RepGrid has been used for testing or extending theories such as value-in-use [42], determining factors that cause users to ignore on-line marketing messages [43], understanding educators' personal beliefs regarding education and learning [44], and students' perception of the usefulness of management frameworks such as Porter's Five Forces, SWOT analysis, and the Resource Based View [45].

It is important to note that RepGrid has been highly modified in some prior research, sometimes with detrimental effects. In order to compare multiple grids,

the data has to be normalized so all grids contain the same constructs. This means that either content analysis needs to be performed on individual grids (which exposes the data to an influence from the researcher), or constructs have to be supplied (which loses the richness of the data). Napier et al. [21] is a good example of the former, while Write et al. [45] illustrates the latter.

With the complexity of RepGrids and importance of appropriately designing RepGrid studies, it may seem impossible for researchers to get it right. We followed guidance provided in key RepGrid reference books [46], [47] and journal articles that provide guidance on how to adapt RepGrid to IS research [40], [48]. Following well established guidelines such as those provided by Fransella et al. [47]; Jankowicz [46]; Tan and Hunter [48]; Curtis et al. [40]; and Kelly [34], this paper describes a grounded research study completely based on the repertory grid technique.

RepGrid studies exploit the fact that subjects describe a *topic* in their own words, as they perceive it. To accomplish this, interviewees are first asked to name several *elements*. In our study, "elements" were individuals who have performed the incident response role. Ideal and incompetent 'anchors' were then provided in order to help aid the comparisons [49]. During each interview, three elements were randomly chosen to elicit *constructs* from each subject. This was accomplished by asking a subject, "In terms of the topic, how are two of these elements alike, but different from the third?" The subject (S) was encouraged to give two dichotomous, polar answers. In some instances, we had to help S refine constructs by *laddering,* or further narrowing the focus of the elicited answer to be related to the topic. For example, laddering may be effective if an interviewee is asked to compare vehicles they are considering purchasing. If S responded "two of them are red, and one is blue", the answer yields nothing about S's preferences. The interviewer would use a laddering technique by asking a question such as "What is it about the color that influences your buying decision?" Now S might answer with a better response such as "Red is a brighter color, and blue is not very cheerful". If not, further laddering would be necessary.

After constructs were elicited (14 – 17 constructs were normally elicited within an hour), S was asked to provide a numerical ranking for how well each construct (skill) describes the element (peer). In the above example, the respondent would be asked "On a scale from 1-6, where one is bright, and five is not cheerful, please provide a rating for each vehicle you were considering purchasing". This continued until the entire grid was completed.

4. Data

Five security incident managers participated in our exploratory project to test the feasibility of remotely using RepGrid in a video teleconferencing environment and to provide data for an exploratory study. The interviewees' experience ranged from 3 to 20 years in InfoSec related fields (with an average of 13.4 years). The highest level of education of one S was high school, another had a bachelor's degree, three had master's degrees. All worked at a Fortune 500 company with over 70,000 employees and over $49 billion in revenue. Each interviewee provided 14 to 17 constructs.

Semi-structured interviews, which were approved by the institutional review board, followed a scripted interview protocol and were conducted using the WebEx MeetingPlace teleconferencing service. The researcher explained the purpose of the study, provided an overview of the RepGrid technique, and explained informed consent. S's were then asked demographic questions about the organization they work for, number of years' experience they have in incident response, level of education, and other background information.

During the interview, an Excel spreadsheet was shared over the WebEx session with each interviewee, and S was asked to list six security incident responders he or she has worked with (this was combined with an ideal and incompetent anchor). S was given the option to use initials, numbers, or other codes for individuals if they preferred to keep names anonymous. These elements were listed at the top of the spreadsheet. Once incident managers were identified, another worksheet was displayed which randomly highlighted incident responders to compare.

S was then asked to name characteristics that were shared between two individuals (elements) but that differed from the third (this generated interviewee-solicited constructs), in an attempt to elicit polar opposites. For example, they might have said A and B are both hard workers but C often arrives late. This process was repeated until S could no longer identify any new constructs. The interviewee was then asked to rate each individual on a scale from 1-6 to indicate which construct in the pair better described that individual (1 being the value on the polar left and 6 being the value on the polar right). Interviewees were finally asked to stack rank each individual for their overall success as an incident response manager.

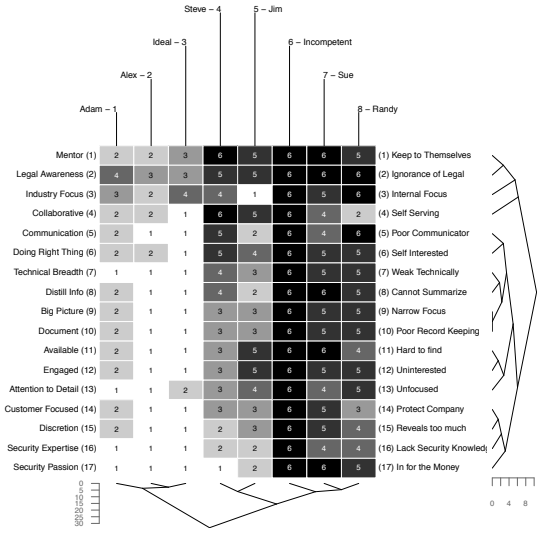

Figure 1 Individual RepGrid

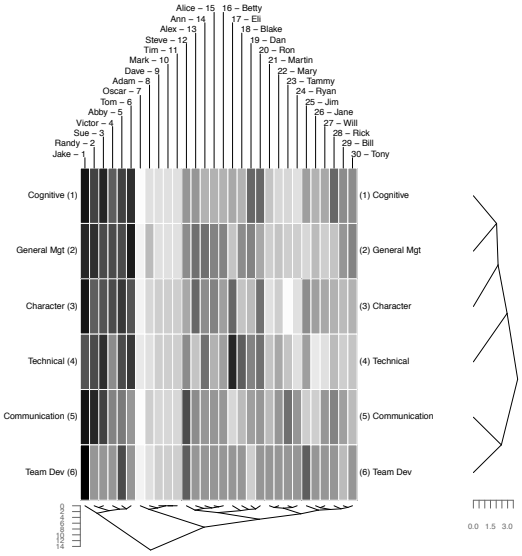

Figure 2 Aggregate RepGrid

5. Analysis

The data was analyzed with custom code written by one of the authors in the R statistical programming language. This code used the OpenRepGrid and Principle Component Analysis (PCA) libraries. Individual grids were created for each interviewee as shown in Figure 1 above.

Anonymized elements (individual InfoSec incident responders) are listed at the top of the grid and the elicited constructs are listed on the left and right. This format of displaying grid data was adopted from Bertin [50]. The constructs and elements were re-ordered to facilitate clustering and each cell was shaded to correspond with its score. Dick [51] provided some guidance on validating RepGrid based on shading of clusters. For example, elements with similar meanings are likely to be shaded similarly. In our data, customer focus, discretion, security expertise, and a passion for security are highly correlated. An element that is almost uniformly light or dark may be valid for the comparison from which it was elicited, but may not be useful in the comparative case. In our data, legal awareness and mentoring are both consistently shaded, suggesting that while this attribute may be important, in this dataset it is not useful for making a distinction across elements. In other cases, clusters of elements may become apparent, with the elements on the left highly correlated with the first few constructs and elements on the right highly correlated with elements on the bottom. This might represent polarity or a natural segmentation of the elements.

While evaluating individual data is interesting, it contributes little to an organizational or industry-wide understanding of the incident response role. In order to compare grids, elicited constructs must be uniformly coded. Thus, after the interviews were performed, a unified list of elements was created. The elements of this list were then iteratively coded in order to group similar concepts. This step minimized the grid dimensions and provided a method for cross-grid comparison. Once the categorical classifications were determined, a weighted average of each grouping was determined by calculating the mean of the product ratings that described how well the construct describes the individual by the forced ranking of the individual.

Table 1 above lists the skills that were elicited during the interviews, the categories we identified for each group of skills, and the weighted success factor for each group.

The values for the categorical constructs were then normalized using an average value for each skill for each interview. This aggregate grid was then analyzed and is displayed in Figure 2 above.

In Figure 2 the data shows a high correlation between Cognitive skills (attention to detail, seeing the big picture, ability to distill information), General Management skills, and elements of Character. Likewise, Team Development, and Communication skills are closely related.

Table 1 Incident Response Skill and Categories

Category	Rank Value	Constructs	
Character/Integrity	0.96	Customer Focused	Self-Starter
		Discretion	Self-Improvement
		Security Passion	Efficient
Cognitive	0.91	Attention to Detail	Organize Thoughts
		Big Picture	
		Ability to Distill Info	
Communication	0.56	Clearly Communicates	Clear Written Communication
		Presents Well	Active Listener
General Management	0.77	Industry Focus	Influence
		Ability to Document	Understand Power Structure
		Process Knowledge	
		Organized	
Leadership/Team Dev	0.45	Collaborates	Available for Others
		Mentor	
		Team Building (Process)	
Technical	0.60	Technical Breadth	Networking
		Security Expertise	Programming
		Legal Awareness	
		Certifications	

We then grouped individuals (using Ward's distance) based on the similarity of the categorical constructs. We subsequently performed a hierarchical cluster analysis to group elements into similar groups. This is graphically displayed in the dendrogram provided in Figure 3. In this figure we are able to see 4 to 5 clusters of individuals (elements) that are similarly represented by their constructs.

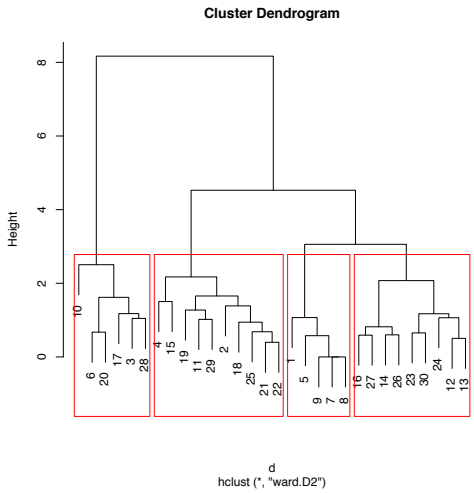

Figure 3: Dendrogram and clusters of incident responders

To develop archetypes for the data, we first calculated a Z-score (deviation from the mean) for each incident responder identified during the interview. The average Z-score for each incident responder in that cluster was calculated to provide a numerical representation for each construct in the cluster. The Z-scores were then plotted on a star chart as shown below in Figures 4-7.

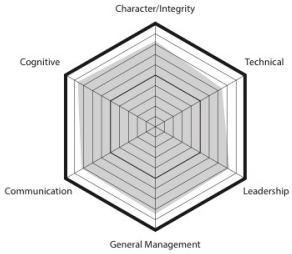

Figure 4: Archetype I

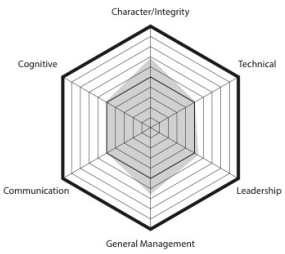

Figure 5: Archetype II

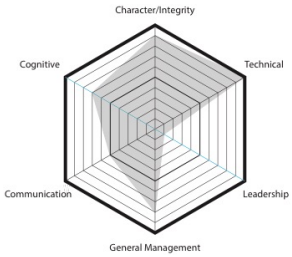

Figure 6: Archetype III

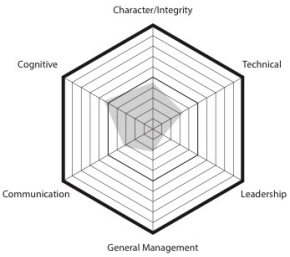

Figure 7: Archetype IV

6. Findings

Managers in almost every industry are struggling to build effective incident response teams and there is no consensus regarding the skills needed. This may be because there is no single incident response role and no individual has every skill that a response team may require. This study helps identify the most important

skills needed on a team and clusters of complementary skills in the individual. We also see that teams are assembled from archetypes that complement one another.

Our results identified character and integrity as the most important attribute influencing an individual's success as an incident responder. However, these categories were identified in only two prior studies. Another category of skills, which is highly correlated with an individual's success, included problem solving skills. This was identified in all four prior studies. Aspects of leadership and collaboration were identified in three prior studies, but were found to be the least significant factors related to success in our data.

In this study we identified four archetypes of the incident responder shown in figures 4-7. We interpreted these archetypes to represent balanced high performers, project managers, technical investigator, and security advocates.

6.1 Archetype I: Balanced High Performer

Surprisingly, our analysis revealed one archetype — which scored far above average in almost every category. We refer to this archetype as "Balanced High Performer" because while the individuals may not have exhibited a high association with specific skills in their individual grids, when the skills were aggregated into categorical values, the high performer tends to have all the bases covered. Interestingly, our sample indicates that while the high performer typically scores way above the mean for technical skills, this value is slightly lower than the other categories. The mean ranking for individuals in this archetype is a 5.2 out of 6.0.

6.2 Archetype II: Project Manager

The second archetype tends to have general management skills and character/integrity exceeding the mean values. Other attributes are close to the mean. The incident responders identified during interviews were not people managers; yet a specific archetype emerged where general management skills and character/ integrity were important. The mean ranking for individuals in this archetype is a 3.4 out of 6.0.

6.3 Archetype III: Technical Investigator

The third archetype that emerged is a technical leader. The skillset of the Technical Expert is obviously dominated by their far superior technical abilities, but they also have high character/integrity and general management skills. However, the technical leader tended to score far below average on leadership attributes and seems to be an average communicator, resulting in a less effective incident responder. The mean ranking for individuals in this archetype is a 3.7 out of 6.0 slightly higher than the project manager.

6.3 Archetype IV: Security Advocate

We label the final archetype "Security Advocate." This individual seems to have the ability to both see the big picture and pay attention to detail. This individual is also able to distill information and is customer focused. These skills individually rank very high. However, it seems that leadership and general management skills appear to be weaker. The mean ranking for individuals in this archetype is below the mean, with a 2.0 out of 6.0.

7. Discussion

An individual's skills may be fairly generic and applicable to almost any task, or be highly specific to a firm, occupation, or industry [52]. Academic programs can draw on the research presented here to help shape their information security curriculum. Managers can use these findings to better hire and train their incident response staff members.

This study contributes to the resource based view by identifying configurations of skills or capabilities that are uniquely present in individuals who are deemed most successful in their InfoSec incident response roles. Further research is needed to validate the archetypes in organizations and to determine how they fit into organizations' hiring practices. If incident response roles have indeed become specialized, then a successful team might contain a balance of these "specialties." Future studies are needed to determine optimal skillsets across members of a single team. Further research into how skills identified for an incident responder in general load onto the specialized roles would also be helpful.

In summary, we answered the following research questions in the following ways:

RQ1: What general and specialist skills or capabilities are needed for an InfoSec response team to effectively respond to incidents?

Table 1 lists the individual skills that were elicited from the incident responders during our interviews. This table also provides the qualitative categories (Character, Cognitive, General Management, Technical Skills, Communication, Team Development) that were used to code these skills into general categories.

RQ2: What is the relative importance of these skills for an individual to be successful in the incident response role?

As shown in table 1, our analysis shows that a focus on the customer or end-user, a passion for security, attention to detail and seeing the big picture are evident

in the most successful incident responders, while the abilities to define processes and to mentor others was apparently not highly important for high-performing incident responders.

RQ3: What sets of skills or capacities (configuration of complementary skills) are possessed by individual incident responders?

Incident response teams must be capable of carrying out a variety of diverse tasks. Different incident responders possess subsets of technical, managerial, communication and other skills that define distinct archetypes. While these capabilities are shared between archetypes, their configuration makes individuals with specific configurations better suited for specific roles within the organization.

Successful incident responders in our study tend to have *some* skills in *each* category (even if they do not possess *all* skills in any particular category). However, given the difficulty to find an ideal candidate, the technical investigator seems to perform slightly better in the incident response role than the project manager.

When ranked individually, character/integrity (a passion for security, self-starter, customer focus, etc.) and cognitive skills (seeing the big picture, ability to analyze problems, etc.) were the top two most important skillsets. However, individuals who have these characteristics but lack technical, leadership or general management skills (all of which are complementary capabilities) are not successful in the incident response role. Incident managers with high character/integrity and high general management skills, yet only moderate levels of other skills, tend to be more competent.

8. Conclusion

This paper examines the skills that information security incident responders have identified in their peers. Our study findings indicate that the incident response role is similar to that of a project manager and IS technician, but also embodies unique configurations of skills which are not success factors for either of those roles. By viewing these skills as strategic resources, we begin to understand the complementary nature they have on one another. This is the first paper that we know of that has made an attempt to demonstrate the complementary nature of skills in IS research. While it may be generally concluded through inductive reasoning that communication skills are present in individuals that are successful in a variety of ICT roles and that communication skills must be combined with technical competencies in the specific area, there has been no study that has attempted to identify the exact nature of this complementary relationship.

This has important implication to both theory and practice. It provides evidence that the Theory of Resource Complementarity applies to knowledge based workers. Specifically, the configuration of skills has a direct effect on how successful individuals are in carrying out specific assignments. Managers should attempt to hire individuals with specific combinations of skills. When unsuccessful in finding an ideal candidate, managers should prioritize their training efforts based on both the importance of each skill on its own and in combination with others.

The RepGrid technique is also designed to elicit bi-polar constructs which identify differences between elements. When an attribute such as "knowledge about current hacking events" is important to a role, it might not be identified if all incident responders (successful or not) have that trait. Using an incompetent anchor mitigates this methodological limitation to some extent, but does not eliminate it. We further note that this study was conducted with individuals in various incident response roles in one large organization. This study needs to be extended to include other organizations to determine if similar archetypes develop in the industry. Several organizations have already agreed to participate in such a follow-on study. A general survey based on the elicited skills could also be beneficial, to provide further evidence of the prioritization of skills and provide empirical evidence (through factor analysis) that the categories we used to code these skills are valid.

This paper is an important first step in recognizing that skills and characteristics cannot be prioritized individually in staffing or development decisions. By recognizing there are specific configurations of skills that enable individuals to be successful as incident responders, managers and researchers can begin to understand how to address the present situation where there are not enough cyber security professionals to fill the needs of the industry — especially in the incident response role.

9. References

[1] FIRST, "Alphabetical list of FIRST Members," Jan-2016. [Online]. Available: https://www.first.org/members/teams. [Accessed: 14-Mar-2016].

[2] FIRST, "FIRST History," 2016. [Online]. Available: https://www.first.org/about/history. [Accessed: 14-Mar-2016].

[3] ISACA, "State of Cybersecurity: Implications for 2016," ISACA, Rolling Meadows, IL, Feb. 2016.

[4] R. Bejtlich, J. Steven, and G. Peterson, "Directions in incident detection and response," *IEEE Security & Privacy*, no. 1, pp. 91–92, 2011.

[5] R. Ruefle, A. Dorofee, D. Mundie, A. D. Householder, M. Murray, and S. J. Perl, "Computer

security incident response team development and evolution," *IEEE Security & Privacy*, vol. 12, no. 5, pp. 16–26, 2014.
[6] M. Nowruzi, H. H. Jazi, M. Dehghan, M. Shahmoradi, S. H. Hashemi, and M. Babaeizadeh, "A comprehensive classification of incident handling information," presented at the Telecommunications (IST), 2012 Sixth International Symposium on, 2012, pp. 1071–1075.
[7] Bureau of Labor Statistics, "Occupational Outlook Handbook, 2016-17 Edition," U.S. Department of Labor, Washington DC, Dec. 2015.
[8] J. Barney, "Firm Resources and Sustained Competitive Advantage," *Journal of Management*, vol. 17, no. 1, pp. 99–120, Mar. 1991.
[9] B. Wernerfelt, "A resource-based view of the firm," *Strategic Management Journal*, vol. 5, no. 2, pp. 171–180, 1984.
[10] P. Milgrom and J. Roberts, "The economics of modern manufacturing: Technology, strategy, and organization," *The American Economic Review*, pp. 511–528, 1990.
[11] S. Nevo and M. Wade, "Firm-level benefits of IT-enabled resources: A conceptual extension and an empirical assessment," *The Journal of Strategic Information Systems*, vol. 20, no. 4, pp. 403–418, 2011.
[12] S. Nevo and M. R. Wade, "The formation and value of IT-enabled resources: antecedents and consequences of synergistic relationships," *MIS Quarterly*, vol. 34, no. 1, pp. 163–183, 2010.
[13] D. J. Teece, "Profiting from technological innovation: Implications for integration, collaboration, licensing and public policy," *Research policy*, vol. 15, no. 6, pp. 285–305, 1986.
[14] SEI, "What Skills Are Needed When Staffing Your CSIRT?," May-2015. [Online]. Available: http://www.cert.org/incident-management/csirt-development/csirt-staffing.cfm? [Accessed: 15-Mar-2016].
[15] SC Magazine, "Skills in demand: Incident response specialists," *SC Magazine*, 2014. [Online]. Available: http://www.scmagazine.com/opinions/skills-in-demand-incident-response-specialists. [Accessed: 15-Mar-2016].
[16] R. McMillan and A. Walls, "Seven Steps to Creating an Effective Computer Security Incident Response Team," Gartner Group, Stamford, CT, G00225512, Mar. 2016.
[17] T. R. Chen, D. B. Shore, S. J. Zaccaro, R. S. Dalal, L. E. Tetrick, and A. K. Gorab, "An organizational psychology perspective to examining computer security incident response teams," *IEEE Security & Privacy*, vol. 12, no. 5, pp. 61–67, 2014.
[18] S. C. Sundaramurthy, J. McHugh, X. S. Ou, S. R. Rajagopalan, and M. Wesch, "An anthropological approach to studying CSIRTs," *IEEE Security & Privacy*, no. 5, pp. 52–60, 2014.
[19] D. M. Lee, E. M. Trauth, and D. Farwell, "Critical skills and knowledge requirements of IS professionals: a joint academic/industry investigation," *MIS quarterly*, vol. 19, no. 3, pp. 313–340, 1995.
[20] M. Keil, H. K. Lee, and T. Deng, "Understanding the most critical skills for managing IT projects: A Delphi study of IT project managers," *Information & Management*, vol. 50, no. 7, pp. 398–414, 2013.
[21] N. P. Napier, M. Keil, and F. B. Tan, "IT project managers' construction of successful project management practice: a repertory grid investigation," *Information Systems Journal*, vol. 19, no. 3, pp. 255–282, May 2009.
[22] R. Colomo-Palacios, E. Tovar-Caro, Á. García-Crespo, and J. M. Gómez-Berbís, "Identifying technical competences of IT Professionals: the case of software engineers," in *Professional Advancements and Management Trends in the IT Sector*, IGI Global Spain, 2012, pp. 1–14.
[23] K. Siau, X. Tan, and H. Sheng, "Important characteristics of software development team members: an empirical investigation using Repertory Grid," *Information Systems Journal*, vol. 20, no. 6, pp. 563–580, 2010.
[24] R. J. Mills, N. F. Velasquez, K. J. Fadel, and C. C. Bell, "Examining IS Curriculum Profiles and the IS 2010 Model Curriculum Guidelines in AACSB-Accredited Schools," *Journal of Information Systems Education*, vol. 23, no. 4, p. 417, 2012.
[25] D. Stevens, M. Totaro, and Z. Zhu, "Assessing IT critical skills and revising the MIS curriculum," *Journal of Computer Information Systems*, vol. 51, no. 3, pp. 85–95, 2011.
[26] M.-D. McLaughlin and J. Gogan, "INFOSEC in a Basket, 2004-2013," in *AMCIS*, Savannah, GA, 2014.
[27] E. T. Penrose, *The Theory of the Growth of the Firm*. Wiley, 1951.
[28] K. M. Eisenhardt and J. A. Martin, "Dynamic capabilities: what are they?," *Strategic Management Journal*, vol. 21, no. 10–11, pp. 1105–1121, 2000.
[29] M. A. Peteraf, "The cornerstones of competitive advantage: A resource-based view," *Strategic Management Journal*, vol. 14, no. 3, pp. 179–191, 1993.
[30] R. R. Nelson and S. G. Winter, *An evolutionary theory of economic change*. Cambridge, MA: Harvard University Press, 1982.
[31] R. M. Grant, "Toward a knowledge-based theory of the firm," *Strategic management journal*, vol. 17, no. S2, pp. 109–122, 1996.
[32] G. P. Pisano, "Knowledge, integration, and the locus of learning: An empirical analysis of process development," *Strategic management journal*, vol. 15, no. S1, pp. 85–100, 1994.
[33] G. Schryen, "Revisiting IS business value research: what we already know, what we still need to know, and how we can get there," *European Journal of Information Systems*, vol. 22, no. 2, pp. 139–169, Mar. 2013.
[34] G. Kelly, *The Psychology of Personal Constructs. Volume 2: Clinical Diagnosis and Psychotherapy*. New York, NY: Norton, 1955.

[35] G. A. Kelly, *The Psychology of Personal Constructs. Volume 1: A Theory of Personality*. New York, NY: Norton, 1955.
[36] D. Winter and H. Procter, "Formulation in personal and relational construct psychology," *Formulation in psychology and psychotherapy: making sense of people's problems*, pp. 145–172, 2013.
[37] P. C. Alexander and G. J. Neimeyer, "Constructivism and family therapy," *International Journal of Personal Construct Psychology*, vol. 2, no. 2, pp. 111–121, 1989.
[38] K. E. Weick, *Sensemaking in organizations*, vol. 3. Sage, 1995.
[39] B. M. Walker and D. A. Winter, "The elaboration of personal construct psychology," *Annu. Rev. Psychol.*, vol. 58, pp. 453–477, 2007.
[40] A. M. Curtis, T. M. Wells, T. Higbee, and P. B. Lowry, "An overview and tutorial of the repertory grid technique in information systems research," *Communications of the Association for Information Systems (CAIS)*, vol. 23, no. 3, pp. 37–62, 2008.
[41] C. J. Davis and E. M. Hufnagel, "Through the eyes of experts: A socio-cognitive perspective on the automation of fingerprint work," *Mis Q.*, vol. 31, no. 4, pp. 681–703, Dec. 2007.
[42] F. Lemke, M. Clark, and H. Wilson, "Customer experience quality: an exploration in business and consumer contexts using repertory grid technique," *Journal of the Academy of Marketing Science*, vol. 39, no. 6, pp. 846–869, 2011.
[43] J. Müller, D. Wilmsmann, J. Exeler, M. Buzeck, A. Schmidt, T. Jay, and A. Krüger, "Display blindness: The effect of expectations on attention towards digital signage," in *Pervasive Computing*, Springer, 2009, pp. 1–8.
[44] K. Samuelowicz and J. D. Bain, "Revisiting academics' beliefs about teaching and learning," *Higher education*, vol. 41, no. 3, pp. 299–325, 2001.
[45] R. P. Wright, S. E. Paroutis, and D. P. Blettner, "How useful are the strategic tools we teach in business schools?," *Journal of Management Studies*, vol. 50, no. 1, pp. 92–125, 2013.
[46] D. Jankowicz, *The easy guide to repertory grids*. John wiley & sons, 2005.
[47] F. Fransella, R. Bell, and D. Bannister, *A manual for repertory grid technique*. John Wiley & Sons, 2004.
[48] F. B. Tan and M. G. Hunter, "The repertory grid technique: A method for the study of cognition in information systems," *MIS Quarterly*, vol. 26, no. 1, pp. 39–57, Mar. 2002.
[49] V. Stewart, A. Stewart, and N. Fonda, *Business applications of repertory grid*. McGraw-Hill Companies, 1981.
[50] J. Bertin, *Graphische Semiologie: Diagramme, Netze, Karten*. Walter de Gruyter, 1974.
[51] M. Dick, "The Use of Narrative Grid Interviews in Psychological Mobility Research," in *Forum Qualitative Sozialforschung/Forum: Qualitative Social Research*, 2000, vol. 1.
[52] B. F. Ingram and G. R. Neumann, "The returns to skill," *Labour economics*, vol. 13, no. 1, pp. 35–59, 2006.

Appendix 1: Overview of incident response skills identified in prior publications

SEI		SC Magazine		Chen		Gartner
Personal Skills	Communication (Written and Oral)	Cognitive	Learning Ability	Routine Events	Investigative skills	Technical Systems Knowledge
	Presentation Skills		Problem Solving Skills		A desire to acquire/share new knowledge	Technical Artifact Knowledge
	Diplomacy		Investigative Skills		The ability to problem-solve	Investigation Process Capabilities
	Ability to follow process and procedures		Intelligence		Curiosity	Intelligence Analysis Capabilities
	Team skills		Decision-Making Competence		Attention to detail	Incident Supervision
	Integrity	Character	Work Ethic		Detect patterns in routine material or data	Communications Management
	Knowing One's Limits		Specific Curiosity		Perceive something is wrong or likely to go wrong	Public Relations and Media Management
	Coping with Stress		Resilience		Rapidly compare data accurately	Law Enforcement Liaison
	Problem Solving		Self-motivate	Non-Routine	Information-sharing skills	Legal and Compliance
	Time Management		Detail Oriented		Collaboration skills	HR Management
Technical Skills	Security Principles		Proactive		A preference for working with others	Planning and Evaluation
	Security Vulnerabilities/ weaknesses		Adaptive			
	The Internet		Perseverance			
	Risk Analysis		Diverse Curiosity			
	Network Protocols		Ambiguity Tolerance			
	Network Applications and Services	Social/Team	Trustworthiness			
	Network Security Issues		Collaborative Problem Solving			
	Host/System Security Issues		Motivation to work on behalf of the team			
	Malicious Code (Viruses, Worms, Trojans)		Communication Skills			
	Programming Skills		Mentoring/Coaching ability			
Local Procedures	Understanding/ Identifying Intruder Techniques					
	Communication Policies (encryption use)					
	Incident Analysis					
	Maintenance of Incident Records					
(SEI 2015)		(SC Magazine 2014)		(Chen et al. 2014)		(McMillan and Walls 2016)