6-2013

Complementary Resource Effects Across Organizational Boundaries and the Remediation of Security Incidents

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

Janis Gogan
Bentley University, USA, jgogan@bentley.edu

26th Bled eConference

eInnovations:
Challenges and Impacts for Individuals, Organizations and Society

June 9, 2013 – June 13, 2013; Bled, Slovenia

Complementary Resource Effects Across Organizational Boundaries and the Remediation of Security Incidents

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

Janis Gogan
Bentley University, USA
jgogan@bentley.edu

Abstract

Organizations experience frequent cyber-attacks, and recovery comes at a high cost. Of especially high concern are those breaches involving inter-organizational networks, since repercussions can quickly spread across organizations. We report on a case study of such a security incident. Inter-organizational cooperation was required to detect the scope of the breach and to recover from its effects. Drawing on the resource based view (RBV), we propose that effective response to security incidents relies on bundles of complementary resources (assets and capabilities) available to the cooperating parties. We identify institutional, technical, and organizational resources used during incident response, and analyze to what extent each was complementary to or non-compatible with other resources. Our findings suggest that resources can be complementary in some situations and not complementary in other situations. We identify specific forms of non-compatibility, and offer suggestions for further research which would aim to help organizations assemble resource bundles to effectively respond to network breaches that can impact inter-organizational relationships.

Keywords: Resource Based View, Complementary Resources, Interorganizational Collaboration, Network Security, Incident Response

1 Introduction

In 2011, large organizations reportedly spent on average 6.5 million Euro recovering from security breaches, and took 18 days to recover from such incidents (Ponemon Institute, 2011). Valid username and password combinations ("credentials") provide access to an organization's intellectual property, and are thus highly valued in black-market exchanges. One study reported that individuals are likely to use the same username and password combination on fifty-four per cent of sites they visit (Bang, et al., 2012). Knowing this,

malicious parties harvest as many credentials as possible. Attacks using stolen credentials are difficult to detect because their usage behavior appears legitimate.

Prior IS security studies addressed questions such as: Why do some individuals use more secure passwords, while others do not (Duggan, et al., 2012)? How strong are user passwords and how often are they forgotten (Florencio & Herley, 2007)? or How can organizations apply social pressure and penalties in order to enhance end users' security awareness (Boss, et al., 2009) (Herath & Rao, 2009) (Johnston & Warkentin, 2010)? Other studies examined how organizations protect themselves (Hu, et al., 2007) (Temizkan, et al., 2012), end-users' motivations and security-related behavior (Liang & Xue, 2010) (Guo, et al., 2011), and the motivations of malicious agents (Mookerjee, et al., 2011) (Galbreth & Shor, 2010). Thus far, few studies have examined IS security issues at an inter-organizational level, yet during network security incidents, an organization, seeking to identify what has occurred and how to recover from attacks may need to cooperate (Liu, et al., 2011) or share information with other firms (Gal-Or & Ghose, 2005).

We conducted a case study to investigate whether, to what extent, and how bundles of complementary institutional, technical, and organizational resources facilitated inter-organizational cooperation in response to security breaches. A similar classification scheme has been applied in other studies of interorganizational collaboration (Fedorowicz et al., 2006; Gogan & McLaughlin, 2013).

Our study examined how two organizations –members of the Nordic DataGrid Facility (NDGF) – collaborated to investigate and remediate a security breach that occurred at the University of Oslo (Universitetet i Oslo, UiO). We analyzed this security incident by examining how bundles of complementary and non-compatible resources facilitated or impeded members' responses to the breach.

In the next section, we discuss relevant studies in three research streams: IS security, the resource based view of strategic management and industrial organizations, and IS studies that drew on RBV. We focus on prior research that examined how bundles of complementary resources support operational and strategic effectiveness.

2 Complementary Resources in IT Security Programs

The strategic management of resources is a core topic in management research. Early studies of the resource based view of the firm (RBV) examined how resources contribute to competitive advantage (Wernerfelt, 1984) (Barney, 1991). Subsequent studies examined how resource bundles and/or dynamically reconfigured capabilities support competitive advantage (Eisenhardt & Martin, 2000). Studies in the last five years have applied RBV to such varied topics as strategy in small to medium size enterprises (SMEs), how firms use shared resources to compete effectively in global markets (Mesquita & Lazzarini, 2008), management of human capital (Ployhart, Van Iddekinge, & Mackenzie, 2011), and how knowledge resources are managed in technology-enabled social networks (von Krogh, 2012).

A complementary relationship may be thought of as "the whole is more than the sum of its parts" (Aristotle, cira 350 BC). According to economists, resources are complements when a firm's profit function satisfies increasing differences from combining multiple resources (Milgrom & Roberts, 1990). To be considered complementary, resources must also satisfy the restriction of "supermodularity" or they demonstrate increasing differences in the output of the resource configuration when either resource is increased (Milgrom & Roberts, 1995). Thus, economic studies of supermodularity provide a mathematical construct which enhances the understanding of how managed resource bundles affect firm outputs—an increase in either resource will yield increasing realized values of the bundled set of resources.

Studies by Milgrom (1995), Bresnahan (2002), Brynjolfsson (2002), Hitt (2007), and McAfee (2008) examined the management and use of complementary resources. Nevo and Wade (2010) and (2011), extended this research by drawing on systems theory (Corning, 1998). Nevo and Wade identified necessary preconditions through which the advantages of complementarity can be realized. They assert that a firm will not realize increasing gains of two resources if those resources are not compatible, and they add a further restriction: gains from complementarity must offset the additional costs of resource integration.

Studies of managerial aspects of IT/IS security programs have focused on several aspects, including the technical performance of various security technologies (Cavusoglu, Mishra, & Raghunathan, 2004), deterrents of security incidents that result from IT misuse (D'Arcy, et al., 2009), effectiveness of various preventive measures (Yue & Cakanyildirim, 2007) and maintenance efforts required to sustain preventive measures (Mookerjee et al., 2011). Numerous practitioners remind us that investments in up-to-date resources such as intrusion protection systems (IPS), vulnerability scanners, and highly trained security engineers will not prevent all security incidents from occurring. Many IS managers do not feel that their security challenges are due to insufficient investment in security equipment, policies, or people; rather, it is the complexity of their environments which hinders their efforts to prevent security incidents and respond to them (Richardson, 2011). To date, there has not been extensive research on how firms actually respond to security incidents—perhaps because many organizations are reluctant to not publically report such incidents.

The resource based view has proved to be a useful lens to study strategic and operational management, and it should prove similarly useful in shedding light on the effective configuration of assets and capabilities for IT and IS security programs. Thus far, however, RBV has not been extensively applied to IS security research. Our research seeks to fill that gap by investigating how bundles of complementary and non-compatible resources affect organizations' ability to respond, singularly or collectively, to security incidents.

3 Research Methodology: Case Study

The Computing Emergency Response Team (CERT) at the University of Oslo (Universitetet I Oslo, UiO), is responsible for detecting, responding to, and remediating security incidents that affect the university. At 18:34, on 9 August 2011, one of UiO's high performance computational grids was taken off-line because it was discovered that it was compromised by a malicious agent. Data about this incident and the resources involved in detection and

remediation were gathered from public and private sources (presentations, web site, etc.) and interviews conducted with four individuals:

- manager of the UiO Computer Emergency Response Team in Oslo, Norway
- security officer at National Supercomputer Centre at Linköping University in Sweden
- technical leader in Cisco's Threat Research in Austin, Texas, USA
- engineer in Cisco's Security Research and Operations team in Austin, Texas, USA

Interviews were conducted via WebEx sessions, e-mail, and instant messenger conversations. Analysis proceeded with the authors independently assigning codes using a high-level coding scheme. Specifically, each author sought evidence for the existence of, and impact of several categories of resources:

- institutional assets (e.g., funding agencies, laws or regulations)
- institutional capabilities (e.g., professionally sanctioned methodologies)
- IT assets (e.g., hardware, software, data, network)
- IT capabilities (e.g., change management, programming language facility)
- organizational assets (e.g., reputation, cash resources)
- organizational capabilities (e.g., training, governance, collaboration track record)

The authors jointly reviewed the interview data to reach consensus on these and other codes. A grounded interpretive lens was then used to consider whether each resource acted as a complement, substitute, or was non-complementary with other resources in the bundle as it related to the investigation and remediation of the security incident.

4 Findings

4.1 A Security Incident: Password Harvesting at UiO

Almost a year before the attacks were discovered, on 18 October 2010, a security researcher released information on a vulnerability in the C software compiler included in most Linux operating systems. This vulnerability could be used by an authenticated user to escalate their privileges to that of system administrator[1]. The security advisory included proof-of-concept code that could be used in an attack. On 21 October 2010, Cisco released an IntelliShield alert[2] which explained the vulnerability and indicated it was unlikely to be used in an attack. However, in November 2010, UiO's operations team received notification that the vulnerability had been exploited to compromise computational grids at other facilities.

In the middle of the night, 23 June 2011, an attacker used a researcher's credentials (obtained from another university) and used the vulnerability described in the October 2010 security

1 For details of this vulnerability see http://seclists.org/fulldisclosure/2010/Oct/257
2 The alert is available at http://tools.cisco.com/security/center/viewAlert.x?alertId=21646

advisory to gain administrative access to one of UiO's login node on their computational grid. Once they obtained access to this node, the attacker compiled a modified version of the SSH[3] application to record other usernames and passwords combinations and store the SSH keys[4] used to access the system. The attacker was also clever enough to compile a backdoor[5] into the SSH application, ensuring they could retain access even if all user passwords were reset.

On 24 June, the attacker compromised a second login node and the SSH program on that node was also recompiled to steal more usernames and passwords. On 15 July, the grid's master node was compromised. The attackers actions remained unnoticed until 9 August 2011, when the UiO Operations team notified the university CERT team of abnormal behavior they observed in the SSH application. The grid was immediately taken off-line, and investigation into the incident began. At 17:45, UniNETT (the network that connects most Norwegian universities) was notified of the outage. At 18:34 all the grid partners received electronic notifications of the outage. Normal operations were resumed on 12 August 2011 and the investigation concluded shortly after.

Between August 9 and 12 2011, staff at UiO and National Supercomputer Centre exchanged emails, describing their interpretations of data contained in netflow[6] and local system logs.

The UiO CERT team had followed best practices in incident response and recovery. In order to maintain a record of the account, they created disk images before reinstalling the compromised nodes. The team also performed security scans and penetration tests against the new images in order to verify there were no known vulnerabilities on them.

Staff members at UiO and Linköping University worked together to reconstruct the attack vector. They discovered that on 23 June, the UiO grid was accessed by five users, all participants in an astrophysics research collaboration involving four Norwegian universities and a non-Norwegian university. The CERT team quickly contacted users from the Norwegian universities and ruled them out, as they were using their accounts for legitimate purposes. Our interviews revealed that this was accomplished through a rather simple, informal process that was most likely facilitated by high levels of trust that parties in the Norwegian organizations had with one another, perhaps because of their cultural affinity or prior social and professional relationships. However, the security response team experienced a great deal of frustration in their attempts to get through to a non-Norwegian astrophysicist whose account was used to access the grid at the time of the attack. At that university, the network operations staff were reluctant to share contact information or question the researcher about his actions. Even after the UiO response team contacted this researcher and confirmed that their account had been used to compromise the UiO grid, the security staff at the non-Norwegian university did not acknowledge that their systems had been compromised. Only

3 SSH (Secure Shell) is an encryption application that provides secure access to remote computer systems
4 SSH Keys are used by the SSH application to provide two-factor authentication and increase the security of the connection
5 A backdoor is an undocumented way to access a system that bypasses normal authentication controls.
6 Netflow is a network protocol used to collect data on IP traffic flows. Netflow data is commonly used to in the network traffic analysis and security investigations.

after administrators were given detailed information that proved that the university systems were exploited, did they participate in the investigation and remediation efforts.

5 Resource Analysis

We discuss institutional, IT and organizational resources that were used during the security incident, and how these influenced the discovery of the attack, investigation and remediation. Our analysis proceeded as follows: first, we identified the resources that were utilized during the incident. Each resource was then evaluated as having a complementary, noncomplementary, or substitutive effect on the incident discovery, investigation and remediation processes.

5.1 Complementary Resource

We define a complementary resource consistent with Milgrom, Roberts, Brynolffson, Nevo, Wade and others (as described in the literature review): if adding a resource to a bundle lowers the time required to remediate a security incident, it is complementary. To accommodate the supermodular nature or complementary resources, we must determine if adding more of a resource would further lessen remediation time. This relationship is shown graphically in figure 1.

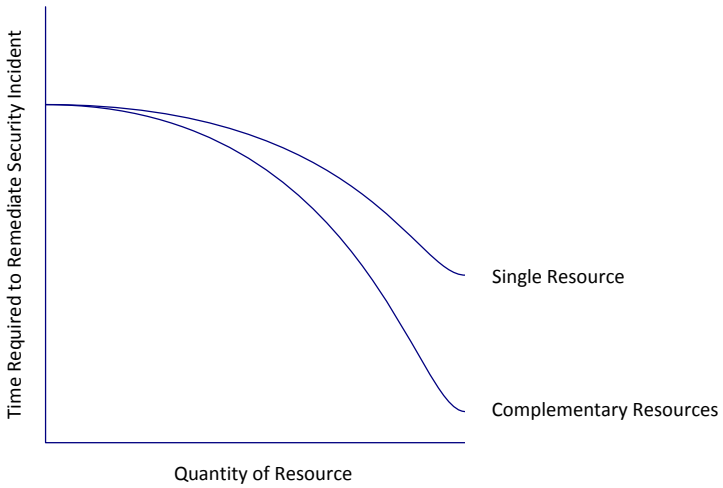

Figure 1: Time Effects of Complementary Resources

5.2 Non-compatible Resource

Resources are not necessarily complementary. We extend the notion of non-compatible resources by classifying these as non-complementary or substitutive in nature.

Non-complementary Resource Some resources have a non-complementary impact on security incident remediation efforts. While these resources may be critical components in an overall bundle and have complementary effects elsewhere, they may negatively impact the time require to remediate a security incident. In order to distinguish from a normal business

obstacle, we also apply the supermodular property to these non-complementary resources: adding more of a resource has a non-linear negative impact. The relationship of non-complementary resources is shown graphically in figure 2.

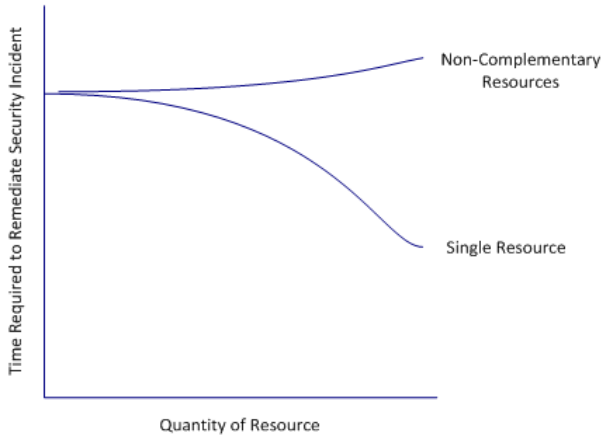

Figure 2: Time Effects of Non-complementary Resources

For example, some technical data and logs are not relevant to a particular security incident. While it is critical to have information about an attack, extraneous, non-filtered data increases the effort required to identify the root cause of an issue.

Substitutive Resource Many resources can be substituted for others. In this case there is no benefit of having substitute resources in a bundle and they are therefore non-compatible resources. While one resource may be more suited for a particular task, and therefore be more effective, the time required for remediation efforts would be exclusive along a curve, unaffected by any substitutive resources in the bundle. This is shown graphically in figure 3. An example of this would be both IDA Pro and OllyDbg—software applications (technical resources) which were commonly used by security response teams when they conducted binary code analysis of malware. While one software package may be more efficient for a particular platform or use, there is no additional time benefit using both.

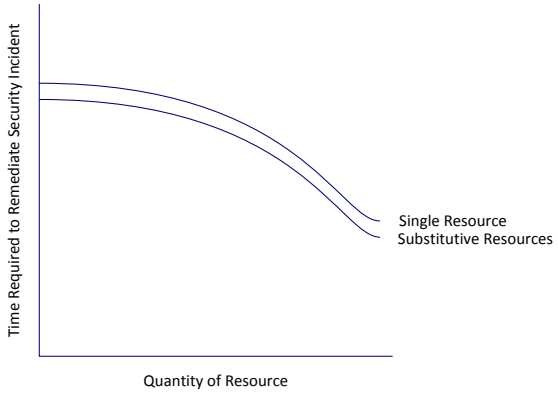

Figure 3: Time Effects of Substitutive Resources

5.3 Resource Analysis

Our analysis identified fourteen resources that were used by or available to the UiO incident response team. We classified these resources as institutional, technical, and organizational and then determined if they had a complementary, non-complementary, or substitutive effect on the response to the security incident described. Table 1 summarizes the resources and their impacts on time needed to investigate and remediate the incident.

		Non-Compatible	
Resource	**Complementary**	**Non-Complementary**	**Substitutive**
Institutional			
Industry Group Involvement	Yes		
UniNETT Network	Yes		
Cooperative Research Agreements		Yes	
Laws Regarding Cybercrime			Yes
Technical			
Security Reports and Notifications		Yes	
System and Network Logs	Yes		
Team Member Skills	Yes		
Grid Facilities			Yes
Security Lab Facilities			Yes
Shared User Database		Yes	
Organizational			
Internal Communication Plans		Yes	
Organizational Structure	Yes		
National and Cultural Similarities	Yes	Yes	
Visual Industry Presence	Yes		

Table 1: Summary of Findings

5.4 Institutional Resources

Industry Group Involvement (Complementary) Involvement in various industry groups is can be costly and time consuming. It is often hard to quantify a return on this investment. UiO and Linköping University were both members of the Forum of Incident Response and Security Teams (FIRST). Their involvement with FIRST provided security training, and members of this team initially met at a FIRST annual meeting. Since they already had a relationship, their involvement in FIRST was critical in reducing the time required to remediate this incident.

UniNETT Network (Complementary) UniNett provided network access to Norwegian schools and universities and its members were notified of outages at other institutions. In this case, notification prompted a staff member at Linköping University to reach out to UiO and offer assistance. The UiO CERT team would not have actively reached out to other organizations for help, as they were capable of handling the incident themselves. However, the additional resources allowed them to focus on root cause analysis while staff at Linköping performed a technical analysis in their lab.

Cooperatives Research Agreements (Non-complementary) A partnership or cooperative agreement that allows researchers at different universities to share computational resources is normally a complementary resource, since organizations share maintenance expenses and costly hardware and software licenses. In this case, the number of partnerships increased the complexity of the investigation and was the source of the attack. Thus, these agreements had a non-complementary effect on the university's security posture; without this relationship the time to remediate the incident would have been zero. It therefore had a non-complementary effect to the remediation efforts.

Laws Regarding Cybercrime (Substitutive) Laws provide a framework for reporting cybercrimes and punishing violators. These laws have the positive externality of producing experts in cybercrime investigation. In the case described here, the attacker was never identified and law enforcement was not notified. Resources that would have been provided to the investigation team were substituted by the team's expertise and knowledge of security. An organization without such resources could utilize law enforcers' expertise.

5.5 Technical Resources

Security Reports and Notifications (Non-complementary) UiO Operations were notified of potential security risks, which could potentially have been complementary to the incident response efforts. When notification was received, the operations team forwarded it to the CERT team, expecting that the CERT team would take appropriate action. However, the CERT team believed that since Operations forwarded the notice, they were handling the issue. Since the notifications were not compatible with the existing process, they had no effect on prevention efforts and added to the complexity of the root cause and remediation efforts.

Relevant System and Network Logs (Complementary) Netflow and system logs provided critical information that helped investigators determine the attack vector used by the attacker and to perform a root cause analysis. Relevant data is a critical component that lessens the time required for remediation and therefore has a complementary effect.

Team Member Skills (Complementary) The UiO CERT and operations teams and staff at Linköping University were highly skilled in different technical areas. The operations team was able to focus on restoring the grid facilities. The CERT team focused their attention on investigating the system logs and contacting other universities. Linköping staff focused on a technical examination of the malware through disassembly efforts and observation of the malware in an isolated security lab (sandbox). These skills were all complementary to the remediation efforts.

Grid Facilities (Substitutive) Once the grid was restored, its computational power could have been used to perform analysis of the malware. Alternatively, some systems could have been used to create a sandbox for analysis. However, this was not necessary as Linköping University already had a security lab setup. Since the grid facility was not used, it had a substitutive effect with Linköping University's security lab facilities.

Security Lab Facilities (Substitutive) Linköping University had a security sandbox that was used to analyze the recompiled SSH program and to examine the logging behavior of the modified SSH application in a safe environment. Investigators also used the lab to identify a backdoor which would have allowed the attacker to regain access even if passwords were changed. This was a highly powerful asset, but having more of them would not provide an increased effect and the analysis could have been done on the disk images (although, the interviews indicate that would not have been nearly as effective).

Shared User Database (Non-complementary*)* As part of the cooperative research agreement, the user database used to access UiO's grid facilities was shared between various organizations. This is necessary for remote users to login and use resources on remote systems. While there may be other technical solutions to share user account data, those would be substitutes when examined in the context of the research agreement. The sharing of the user database had a non-complementary effect on the remediation efforts, for it increased the number of user accounts that were potentially used by the attacker that needed to be investigated; therefore, the shared databases had a non-complementary effect in this context.

5.6 Organizational Resources

Internal Communication Plans (Non-complementary*)* The security communication plan between CERT and Operations was non-complementary. The CERT and operations team did not effectively communicate security risks and remediation efforts. Operations forwarded the notification of the vulnerability to the CERT team and expected CERT to take responsibility for remediation and risk analysis. The CERT team interpreted the forwarded message as an acknowledgement that the issue was being addressed. Lack of a formal communication plan had a non-complementary effect as roles and responsibilities had to be defined during the remediation efforts.

Organizational Structure (Complementary*)* While the UiO operations team could have handled the security incident on their own, they had a dedicated emergency response team, which allowed the CERT team to focus on the investigation and root cause analysis while the operations team focused on remediation. The security expertise of the CERT team provided greater depth and efficiency in the investigation. This expertise and predefined division of responsibilities reduced the time it would have otherwise taken Operations to remediate.

National/cultural similarities (Complementary and Non-complementary) Having cultural similarities is a valuable resource. The relationship and reputation UiO had with other Norwegian schools was complementary. Cultural similarities were not present in the non-Norwegian university which may have hindered some remediation efforts and had a non-complementary effect.

Visual Industry Presence (Complementary) The lead investigator from Linköping had previously given technical presentations about investigating security incidents and issues involved in securing grid systems. He thus built a reputation as an expert and someone that could be trusted. When he reached out to the CERT team at UiO and offered assistance, they readily accepted his help. Thus, time to remediation was positively impacted by this association.

6 Discussion and Suggestions for Further Research

We examined how various resources effected the time required to remediate a network security incident. We identified aspects of a complementary resource paradox: some resources have beneficial or complementary aspects with functional requirements of the IT infrastructure, yet are non-compatible with remediation activities in a security program. We also find that resources that are complementary at one time may not be compatible with resource bundles later on. Our research furthers the understanding of non-compatibility by highlighting the substitutive and non-complementary effects that resources may have when they are bundled.

A limitation of this study is that we focused on time-to-remediation as a dependent variable, whereas a more complete study would include various measures of remediation quality and cost as additional dependent variables.

This is a unique case, with multiple participating organizations. Security resources can support incident prevention, detection, or correction. By assembling different complementary security resources a firm will secure their data and intellectual property. Further research is needed to examine how firms can best collaborate for mutual protection, using complementary assets and capabilities. Further research is needed to gain insights on whether and how resources that help prevent security incidents have a substitutive or noncomplementary impact on incident the detection or on corrective responses.

Our research helps organizations conceptualize how complements, substitutes, and non-complements may affect their security programs. Examining the interaction effects of resources from multiple perspectives may help firms better tackle the security versus usability trade off. In addition, our study reveals that it is helpful to examine the impact of non-compatible resources in one context, weighed against the impact in other contexts. This deeper understanding of assets and capabilities will allow firms to better manage the complexity of the environment, which they identified as the biggest threat to IS security. This increased understanding, from both a functional and security standpoint has the potential to reduce the impact of security incidents that nevertheless will continue to occur.

References

Bang, Y., Lee, D. J., Bae, Y. S., & Ahn, J. H. 2012. Improving information security management: An analysis of ID-password usage and a new login vulnerability measure. ***International Journal of Information Management***, 32(5): 409-418.

Barney, J. 1991. FIRM RESOURCES AND SUSTAINED COMPETITIVE ADVANTAGE. ***Journal of Management***, 17(1): 99-120.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. 2009. If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. ***European Journal of Information Systems***, 18(2): 151-164.

Bresnahan, T. F., Brynjolfsson, E., & Hitt, L. M. 2002. Information technology, workplace organization and the demand for skilled labor: Firm-level evidence. ***Quarterly Journal of Economics***: 339-376.

Cavusoglu, H., Mishra, B., & Raghunathan, S. 2004. A model for evaluating IT security investments. ***Communications of the ACM***, 47(7): 87-92.

Corning, P. A. 1998. "The synergism hypothesis": On the concept of synergy and its role in the evolution of complex systems. ***Journal of Social and Evolutionary Systems***, 21(2): 133-172.

D'Arcy, J., Hovav, A., & Galletta, D. 2009. User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. ***Information Systems Research***, 20(1): 79-98.

Duggan, G. B., Johnson, H., & Grawemeyer, B. 2012. Rational security: Modelling everyday password use. ***International Journal of Human-Computer Studies***, 70(6): 415-431.

Eisenhardt, K. M., & Martin, J. A. 2000. Dynamic capabilities: What are they? ***Strategic Management Journal***, 21(10-11): 1105-1121.

Fedorowicz, J., Gogan, J.L., Williams, C.B. ***The E-Government Collaboration Challenge: Lessons from Five Case Studies.*** IBM Center for the Business of Government, 2006.

Florencio, D., & Herley, C. 2007. ***A large-scale study of web password habits***. Paper presented at the Proceedings of the 16th international conference on World Wide Web.

Gal-Or, E., & Ghose, A. 2005. The economic incentives for sharing security information. ***Information Systems Research***, 16(2): 186-208.

Galbreth, M. R., & Shor, M. 2010. The Impact of Malicious Agents on the Enterprise Software Industry. ***Mis Quarterly***, 34(3): 595-612.

Gogan, J., & McLaughlin, M.-D. 2013. ***Complementary Resources and a Multi-hospital Emergency Medicine System Pilot Test***. Paper presented at the European Conference on Information Systems, Utrecht, Netherlands.

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. 2011. Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model. ***Journal of Management Information Systems***, 28(2): 203-236.

Herath, T., & Rao, H. R. 2009. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. ***Decision Support Systems***, 47(2): 154-165.

Hitt, M. A., Beamish, P. W., Jackson, S. E., & Mathieu, J. E. 2007. Building theoretical and empirical bridges across levels: Multilevel research in management. ***Academy of Management Journal***, 50(6): 1385-1399.

Hu, Q., Hart, P., & Cooke, D. 2007. The role of external and internal influences on information systems security - a neo-institutional perspective. ***Journal of Strategic Information Systems***, 16(2): 153-172.

Johnston, A. C., & Warkentin, M. 2010. Fear Appeals and Information Security Behaviors: An Empirical Study. ***Mis Quarterly***, 34(3): 549-566.

Liang, H., & Xue, Y. 2010. Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective. ***Journal of the Association for Information Systems***, 11(7): 394-413.

Liu, D. P., Ji, Y. H., & Mookerjee, V. 2011. Knowledge sharing and investment decisions in information security. ***Decision Support Systems***, 52(1): 95-107.

McAfee, A., & Brynjolfsson, E. 2008. Investing in the IT that makes a competitive difference. ***Harvard Business Review***, 86(7/8): 98.

Mesquita, L. F., & Lazzarini, S. G. 2008. Horizontal and vertical relationships in developing economies: Implications for SMEs' access to global markets. ***Academy of Management Journal***, 51(2): 359-380.

Milgrom, P., & Roberts, J. 1990. The economics of modern manufacturing: Technology, strategy, and organization. ***The American Economic Review***: 511-528.

Milgrom, P., & Roberts, J. 1995. Complementarities and fit strategy, structure, and organizational change in manufacturing. ***Journal of Accounting and Economics***, 19(2): 179-208.

Mookerjee, V., Mookerjee, R., Bensoussan, A., & Yue, W. T. 2011. When Hackers Talk: Managing Information Security Under Variable Attack Rates and Knowledge Dissemination. ***Information Systems Research***, 22(3): 606-623.

Nevo, S., & Wade, M. 2011. Firm-level benefits of IT-enabled resources: A conceptual extension and an empirical assessment. ***Journal of Strategic Information Systems***, 20(4): 403-418.

Nevo, S., & Wade, M. R. 2010. The Formation And Value Of IT-Enabled Resources: Antecedents And Consequences Of Synergistic Relationships. ***Mis Quarterly***, 34(1): 163-183.

Ployhart, R. E., Van Iddekinge, C. H., & Mackenzie, W. I. 2011. Acquiring And Developing Human Capital In Service Contexts: The Interconnectedness Of Human Capital Resources. ***Academy of Management Journal***, 54(2): 353-368.

Ponemon Institute. 2011. 2012 Cost of Cyber Crime Study: United States.

Richardson, R. 2011. 2010/2011 CSI Computer Crime and Security Survey. In R. Richardson (Ed.): Computer Security Institute.

Salancik, G. R., & Pfeffer, J. 1978. ***The external control of organizations: a resource dependence perspective***: Harper and Row.

Temizkan, O., Kumar, R. L., Park, S., & Subramaniam, C. 2012. Patch Release Behaviors of Software Vendors in Response to Vulnerabilities: An Empirical Analysis. ***Journal of Management Information Systems***, 28(4): 305-337.

von Krogh, G. 2012. How does social software change knowledge management? Toward a strategic research agenda. ***Journal of Strategic Information Systems***, 21(2): 154-164.

Wernerfelt, B. 1984. A Resource-Based View Of The Firm. ***Strategic Management Journal***, 5(2): 171-180.

Yue, W. T., & Cakanyildirim, M. 2007. Intrusion prevention in information systems: Reactive and proactive responses. ***Journal of Management Information Systems***, 24(1): 329-353.