Seven C's of Information Security

Full Paper

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

Janis Gogan
Bentley University
jgogan@bentley.edu

Abstract

The 1991 *United States Federal Sentencing Guidelines for Organizations* (updated in 2004) describes legal requirements for organizations' ethical business procedures. We adapt this framework for the purpose of developing a high-level "Seven C's" framework for ethically-responsible information security (InfoSec) procedures. Informed by the Resource Based View (RBV) of strategic management, we analyze case studies of two organizations to demonstrate the adapted guidelines' applicability. Each organization has a well-established InfoSec program, yet each requires further development according to guidelines in our Seven C's model. We discuss implications for InfoSec policies and standards.

Keywords

Information Security, Ethics, Resource Based View, Federal Sentencing Guidelines.

Introduction

This paper proposes seven guidelines that specify organizational requirements for ethically responsible Information Security (InfoSec) procedures. The guidelines are adapted from the 1991 Federal Sentencing Guidelines for Organizations (updated in 2004 and hereafter in this paper referred to as the Federal Guidelines). Informed by the Resource Based View (RBV) of the firm, we conducted an exploratory two-case study of two mature InfoSec programs, as a first step toward validating the guidelines.

When an organization fails to establish an effective InfoSec program (comprised of appropriate and effective policies, procedures, organizational structures, and financial resources) ramifications can be serious and costly. The average annualized cost of cyberattacks per organization is estimated to be $7.7 million globally; US costs are twice this, at $15.4 million (Ponemon Institute 2015). In one hopeful sign, FIRST (Forum of Incident Response and Security Teams) listed 345 incident response teams in 74 countries (FIRST, 2016a) — nearly double the membership from 2006 (FIRST, 2016b). This is an indication that InfoSec programs are maturing. However, a recent survey reported that only 31% of cybersecurity professionals felt their organizations were well prepared to handle security events (ISACA, 2016). Existing guidance on how to develop a strong InfoSec program is helpful in some aspects, but lacks a high-level, comprehensive explication of the resources (assets and capabilities) needed to support effective programs for preventing, detecting, and responding to InfoSec incidents and challenges.

Research is also needed to better understand how various human, administrative and technical resources interact in effective InfoSec programs. The human resources (especially InfoSec specialists) are expensive (Nowruzi et al. 2012): in 2015, the average salary for an InfoSec analyst was more than $90,000 and demand was expected to grow 18% over the next 20 years (Bureau of Labor Statistics 2015).

This paper evaluates two large well-respected multinational technology vendors' InfoSec policies and procedures in light of InfoSec guidelines ("Seven C's") adapted from the Federal Guidelines. Based on this exploratory two-case study we provide initial evidence that the Federal Guidelines, developed to deter criminally unethical organizational violations, can be usefully adapted to inform organizations' InfoSec policies and procedures. In the two cases, we found strong compliance with some guidelines and weak compliance with others (even at firms considered InfoSec exemplars, there is room for improvement).

The rest of the paper is organized as follows: we present an overview of the resource based view (RBV), the Federal Guidelines, and our InfoSec adaptation. Next, we describe our research method. Then, we

discuss our case study findings applying the adapted Seven C's guidelines to each organization. Lastly, we discuss contributions of our study, limitations and concluding thoughts.

Applying the Resourced Based View (RBV) of the Firm to InfoSec

Penrose (1951) conceived of the firm as a bundle of human, financial, and other resources. According to RBV, optimally configured resources confer strategic advantage (Barney 1991; Peteraf, 1993; Wernerfelt, 1984). InfoSec resources include tangible assets (e.g., computers, networks), intangible assets (e.g., data, software, specialized knowledge), and capabilities (e.g., an engineer's ability to quickly detect a security violation and formulate a response plan) (McLaughlin et al. 2017; McLaughlin and Gogan 2013).

An asset rarely confers an advantage on its own; bundled technical, human, and other assets and capabilities – confer advantages, especially when these resource bundles are unique and difficult to imitate (Grant 1991; Prahalad and Hamel, 1990). Numerous studies reveal that uniquely configured resource bundles account for variations in firm performance (McGahan and Porter, 1997); (Collis and Montgomery 1995). Powell (2001, p. 877) clarifies that "competitive disadvantage is not merely the non-existence of such resources (which would create economic parity)…" However, merely bundling valuable resources will not ensure benefits (Prieto and Easterby-Smith 2006), if a firm lacks the capability to effectively combine valuable resources.

(West and DeCastro, 2001) provide an easily-grasped example: although individual superstars who played baseball for the New York Yankees in the 1980's were rare, valuable, non-substitutable human resources, the team failed to make it to the playoffs from 1982 to 1993, because they did not play effectively together. Therefore, a weakness can sap the strength out of a resource, and the effectiveness of a resource bundle is affected by the extent to which its constituent assets and capabilities are *complementary* (Teece 1986).

When an IT system and related business procedures are not complementary, the system's contribution to organizational performance is inhibited (Bhatt and Grover, 2005; Karahanna et al. 2006; Ray et al. 2005). Conversely, each resource in a bundle may complement or substitute for other resources, which can enhance performance. InfoSec policies, incident response plans, information about specific threats and events, knowledge repositories, and vulnerability databases are helpful InfoSec assets, especially when complementary. InfoSec capabilities such as information-gathering procedures, execution of response plans, or understanding output from security tools also interact in InfoSec resource bundles. Inter-organizational communication channels can complement resources such as InfoSec tools and procedures (Gal-Or and Ghose 2005). Conversely, unpredictable interactions among diverse resources can hinder an organization's efforts to prevent or respond to InfoSec incidents (Beautement et al. 2009; Computer Security Institute 2011). An organization's overall InfoSec capability is also conceptualized as an important high-level resource that impacts customer trust, improved market valuation, business resiliency, and other aspects of performance (Hall et al. 2011). Thus, plans to invest in particular IT resources should take into consideration potentially complementary (or non-complementary) effects on other InfoSec resources as well as on existing IT systems and policies (Berghout and Tan 2013).

Managers assemble and oversee bundles of complementary human, technical, administrative, and other resources to defend against InfoSec incidents and preserve the confidentiality, integrity and availability of IT resources. For example, Cisco's IOS software complements network devices it runs on. Data collected by security controls complement a response team's capability to interpret security logs for rapid response to incidents. An incident response plan should complement an InfoSec team's capabilities; however, thus far few studies have examined how firms build their overall InfoSec capability to prevent, prepare for and respond to specific InfoSec incidents (McLaughlin and Gogan 2014). Many organizations are reluctant to share information about such incidents (Safa and Von Solms 2016; Zietsma et al. 2002).

RBV, a useful lens for shedding light on effective configuration of assets and capabilities for InfoSec programs, has not yet been extensively applied to InfoSec research (Weishäupl et al. 2015). Managerial topics such as the RBV have been underrepresented in InfoSec research, and, case studies have been underutilized in InfoSec research, as a recent literature review observes:

> *"… new case studies need to closely examine whether and how organizations prepare for and respond to InfoSec incidents, and to what extent members of formal incident response teams, and others in and beyond the organization, work effectively to protect resources and preserve*

> *valuable relationships with customers and business partners. This under-studied subject is in need of immediate attention (McLaughlin and Gogan 2017)."*

This exploratory two-case study discussed here addresses that gap by investigating how resource bundles affect InfoSec effectiveness

Federal Sentencing Guidelines for Organizations

The Federal Guidelines, created in 1991 (and updated in November 2004) help judges determine if an organization has acted in an ethically responsible manner (Joseph 2003). Leaders are required to "promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law." The guidelines help judges assess fines for ethical violations, taking into account factors such as the organization's cooperation with prosecutors, acceptance of responsibility, and whether an effective ethics program is in place (Kaplan and Dakin, 1993).

The Federal Guidelines require organizations to demonstrate seven elements of ethical responsibility are present. We see each guideline as pointing to one or more necessary assets or capabilities (resources):

- Compliance standards (assets) and procedures (capabilities) that are judged to be reasonably capable of reducing criminal activity
- Oversight by high-level personnel (capability)
- Due care in delegating substantial discretionary authority (capability)
- Effective communication to all levels of employees (capability)

Reasonable steps to achieve compliance, which include

- Systems for monitoring, auditing and reporting suspected wrongdoing, without fear of reprisal (assets)
- Consistent enforcement of compliance standards including disciplinary mechanisms (capability)
- Reasonable steps to respond to and prevent further similar offenses upon detection of a violation (capability)

We adapted these seven guidelines, as the Seven C's of ethically responsible InfoSec management. Table 1 outlines how the seven Federal Guidelines map to ours. Following this, we discuss prior research published in the AIS Senior Scholars' Basket of journals relevant to each of the seven elements. While we find that some topics (such as employee compliance or non-compliance with InfoSec policies and controls) are widely supported by research in the Basket, many managerially-relevant topics have been understudied. For example, a recent literature review concludes that many studies have investigated issues relevant to incident prevention, but few studies have investigated how organizations prepare for, respond to and learn from InfoSec incidents (McLaughlin and Gogan 2017).

In this paper, we do not attempt to quantify the relative importance of each guideline, but this would be a useful next step in future research.

Compliance: Most organizations define acceptable use of computational resources and data handling, taking into account organizational structure and purpose and specifying sanctions for violations. In some industries regulations require specific polices. For example, the payment card industry (PCI) data security standard (DSS) specifies that organizations conducting business over the internet must undergo annual audits, demonstrating compliance with procedures that ensure the security of personal information. HIPAA requires clinicians to protect the confidentiality of patient records.

Champion: To legitimize an InfoSec policy a high-level sponsor (director, officer, owner) enthusiastically supports it (Dhillon and Torkzadeh 2006), letting employees and external stakeholders see that it is important. A study at the UK National Health Service found that senior management support and ideology influenced both InfoSec management effectiveness and employee awareness (Stahl et al. 2012).

Care: Organizations must not delegate substantial discretionary authority to individuals who are in a position to violate InfoSec policies. Due care may include background checks, NDAs, and mechanisms for restricting access to sensitive data (e.g., require evidence of demonstrable need for access, annually review access controls). Background checks help prevent InfoSec violations (Kwon and Johnson 2013). Since

different roles require different levels of access to sensitive information, the authority to delegate responsibility and other information security related privileges, background checks should occur as individuals are promoted up the organizational hierarchy (Koch et al. 2013).

Federal Guidelines	Seven C's Element	Example
Compliance standards	Compliance	Adhere to regulatory requirements Acceptable use policies Data access and handling policies
Oversight	Champion	Executive sponsor Legitimize the program Signals importance of the program
Due care	Care	Responsible delegation of discretionary authority Background checks, NDAs
Effective communication	Communication	Policies should be distributed and easily accessible Education and training programs
Monitoring, auditing & reporting	Controls	Authentication, Authorizations and Accounting of data Align with compliance (such as legal regulations) Record Keeping
Consistent enforcement	Consistency	Sanctions for violations should be enforced
Respond to and prevent	Correction	Failure analysis Revise failing program elements Revisit appropriate threat and risk models

Table 1:

Seven Federal Guidelines and Seven C's of Ethically Responsible InfoSec Management

Communication: Organizations should conduct training that ensures employees understand and will comply with InfoSec policies. A study involving computer users at eight companies concluded that a security education, training, and awareness (SETA) program is critical to deterring IS misuse by employees (D'Arcy et al. 2009). InfoSec training is reportedly more effective when it relies on learners' systematic cognitive processing of information, is seen as personally relevant, and takes into account learners' previous knowledge (Puhakainen and Siponen 2010). Informal knowledge distribution (distinct from formal methods) influences employees' perceived self-efficacy, which reportedly results in higher levels of employee compliance with organizations' InfoSec policies (Warkentin et al. 2011).

Controls: Organizations should take reasonable steps to ensure compliance with security policies and data privacy laws, such as by using authentication tools and procedures and accounting, and auditing mechanisms. Records need to demonstrate the existence of program elements such as training logs, acknowledgements, etc. High-level reports of violations and methods for getting more detailed information must be part of these controls, because they support transparency as well as discovery for legal prosecution. In addition to technical controls, a mechanism for reporting security weaknesses without fear of retaliation should be provided (such as by directing such reports to a neutral ombudsman).

InfoSec policy compliance "mandatoriness" influences how employees perceive control specification, evaluation, and rewards, which in turn influences the precautions users take (Boss et al. 2009). Bulgurcu *et al.* (2010) clarifies: Rewards do not significantly influence perceived mandatoriness but do significantly influence the perceived benefit of complying with InfoSec rules. A survey revealed that users' attitudes toward InfoSec policies, controls, and sanctions do *not* significantly influence compliance intentions, but perceived risk, work group norms, and work performance do (Guo et al. 2011). Audit logs influence compliance, via identifiability, user awareness, and electronic presence — (Vance et al. 2013).

Controls are potentially-valuable resources, if bundled in complementary configurations. Chen *et al.* (2011) demonstrated (counter-intuitively) that adoption of security standards and other best procedures can weaken an organization's security posture. Systems based on a standard software configuration will contain similar vulnerabilities, so an attacker who identifies how to bypass a control in one organization's system may exploit it in other organizations' standard systems—an event they call "correlated failures." Thus, a helpful preventive tactic is for an organization to diversify its control configurations.

Multiple studies further demonstrate that controls must be implemented with care. A survey showed that subjects tended to underestimate threats, and that sanctions were not very effective in deterring users

from violating InfoSec policies. However, perceived threat severity and coping appraisals may influence employees' intentions to comply (Herath and Rao 2009). To the extent that employees understand InfoSec risks and feel they are competent to deal with them, they are more likely to comply with InfoSec policies. Another study found that sanctions were not influential, and that violators used five "neutralization" techniques to rationalize their behavior: denial of responsibility, denial of injury, denial of the victim, condemnation of the condemners and appeal to higher loyalties (Siponen and Vance 2010).

Consistency: Most experts agree that security policies and procedures should be consistently enforced. General Deterrence Theory, widely used and debated in IS research, states that the perceived certainty, severity, and celerity of a sanction deters users from violating InfoSec policy (Straub 1990). In contexts where policy violations are viewed as morally acceptable, the perceived certainty of getting caught deters users, whereas in contexts in which policy violations are generally viewed as reprehensible, sanction severity has a stronger deterrent effect (D'Arcy et al. 2009). Policies which users perceive as consistently and predictably enforced are reportedly more effective (Vance et al. 2015).

Incident Response (Correction): Once an InfoSec incident is detected, employees should know what to do in order to mitigate the near-term damage. Larger organizations and those that rely heavily on IS (such as eCommerce companies) usually have InfoSec incident response teams in place, while other organizations may incorporate InfoSec incident response checklists into their disaster recovery procedures. Often, a complete response requires notification of stakeholders within and beyond organizational walls.

Disclosure of security vulnerabilities is very important. Wang *et al.* (2013) demonstrated a correlation between risk factors (possible incidents) disclosed in financial reports and actual incidents reported by the media. Similar to Cremonini and Nizovtsev (2010) and Gordon *et al.* (2010), this study revealed that firms that disclose investments in information security have a lower probability of experiencing security incidents, and that the impact of security incidents on stock prices of firms that report security investments is lower than the impact on firms that simply identify security risks.

Once an incident is reasonably resolved, a process of root cause analysis and correction should also be undertaken. Technical controls and/or policies and procedures should be analyzed and modified to prevent reoccurrence. A study of security breaches at TJX and Choicepoint (Culnan and Williams 2009) demonstrated how root cause analysis could identify problematic aspects of an InfoSec program, such as a managerial failure to create a culture of privacy and to ensure accountability. Examining why controls fail, Goldstein *et al.* (2011) tested a *resource weaknesses framework* which they claim aides in investigations into security risks and impacts.

Research Method

We conducted an exploratory two-case study to evaluate our proposed Seven C's InfoSec guidelines. A case study is appropriate for investigating the interplay among issues, technologies, and policies within specific contexts (Yin 2009). We compare and analyze these cases through the 7 C's model, informed by RBV and the theory of resource complements, in a multiple exemplars approach (Denzin 2001). We compare the configurations of resources (assets and capabilities) deployed in each organization, aiming "to enhance generalizability or transferability to other contexts" and "deepen understanding and explanation" (Miles et al. 2013, p. 101) of how complementary resource bundles are configured and deployed in InfoSec programs. We sought to identify and understand technical, administrative, and human resources deployed by each focal organization, and specific resources used by these two organizations for InfoSec incident response. We took into account each organization's institutional context, including how prior InfoSec incidents influenced their existing policies and procedures.

The data for the case study was collected by surveying two organizations with mature security programs. These organizations were selected because of professional relationships the first author had with individuals familiar with each organization's InfoSec policies, procedures, and training programs. Both organizations are considered to be exemplars, in that they have invested heavily in their security programs, are highly regarded by their peers for their ability to execute their security programs, and their programs are often used as models by other organization in the industry.

The author interviewed one individual in each organization, using a semi-structured interview technique in which questions were asked on the seven topics identified in the adapted guidelines, as well as more

generally on the organization's information security policies, procedures, and related topics. We then analyzed the interview transcripts as follows: we manually coded interview segments according to each element of the Seven C's model, and manually open-coded other interview segments that addressed broader topics or substantially different topics.

Both organizations were multinational technology vendors with large hardware and software development efforts, mature security programs, more than 70,000 employees, and revenue in the $50B to $60B range:

- Org X has more than 100,000 employees. A security architect responsible for defining Org X security procedures was interviewed.
- Org Y has more than 70,000 employees. A former employee who was a security architect responsible for defining security procedures at this company was interviewed.

Findings

Although many elements specified in our guidelines were implemented in these two organizations, aspects in need of improvement were also identified.

Org X (>100,000 employees)

Compliance: Many tools are used by Org X teams to report the security posture of their information systems. The tools require that engineers evaluate InfoSec support compliance. However, the compliance system does not check the content of supporting materials, just that supporting information was added. To ensure compliance, an internal audit team spot checks the information produced by these teams.

Champion: Each Org X group is made up of several hundred engineers, responsible for multiple projects. Each group is supposed to have an InfoSec expert who in turn recruits a champion in each team. However, not all groups have designated a security expert and not all security experts have extended their influence down to individual teams. While there is an executive sponsor for information security, some InfoSec champions have support from the executive in their reporting chain, while others do not.

Care: Care of information in and for the InfoSec program is mostly around deciding who is competent and who is not. Central security architects act as gatekeepers who are trusted to be responsible for the overall program. Individuals providing security reports are selected based on their perceived InfoSec competence, as determined by the existing security team. There is no central coordination of care. Security expertise is spread across the organization. Hiring procedures require that the team rely on experts in that team. An informal mentoring program helps less experienced InfoSec team members better understand the impact of the program.

Communication: Our interviewee reported that communication is not very strong in Org X. Information sharing takes place in small clusters of working groups, who get their information from the central team. The central security team at Org X would like to improve communication procedures.

Controls: Teams are expected to comply with specific InfoSec policies, and controls are built into procedures that support the policies. The interviewee at Org X did not elaborate much on these controls.

Consistency: Consistency is a challenge for Org X, and our interviewee noted that they do not have a good solution to address consistency problems. The central security team provides clear instructions on how to test systems for security issues. This team is investigating how to create accurate metrics and reports of controls that support tools used across the organization.

Correction: Correction at Org X is primarily top-down, but changes sometimes do come from the individual contributor level. While team members are committed to making things better, the interviewee noted that it is difficult to determine to what extent corrective measures are effective, because the environment is constantly changing.

Org Y (> 75,000 employees)

Compliance: Org Y uses several tools to track compliance with its security policies. We learned that previously a compliance tool did not force users to provide supporting information before closing

exceptions, and such evidence was usually not provided. Now users are forced to enter such information, and our interviewee reported that it is accurate about 90% of the time.

Champion: The Chief Security Officer is responsible for Org Y's InfoSec program, and *security champions* are expected to execute on initiatives. These individuals are the "eyes and ears into the workings of the teams; they also help raised security issues when teams needed help deciding how best to solve an issue". Security champions are volunteers who are passionate about security. During recent layoffs, some champions were targeted -- they reportedly did not have executive protection/backing/sponsorship.

Care: The Org Y interviewee reported that determining if an individual can be trusted to develop and enforce policy is difficult. The company conducts an initial background check, but does not conduct subsequent background checks. This means that authority to participate in the program largely comes from a person's reputation. The interviewee reported that security initiatives are largely crowdsourced, as there is a massive amount of internal communication between the security champion and others who are passionate about security in internal mailing lists. Some mentoring programs and an internal "security black belt" training program help build credibility within the community.

Communication: Org Y relies heavily on email communication. The interviewee felt email is "a good form of JIT [just in time] communication where questions would be answered quickly (within hours normally)". Org Y tried several times to replace email communications with "social platforms"; but, these reportedly failed because employees at Org Y preferred to keep all communications in a single tool email.

Controls: Like Org X, the Org Y interviewee did not discuss specific controls, except controls used to test, report, and respond to security exceptions. The interviewee claimed that most controls are within the development and implementation standards for security requirements.

Consistency: Consistency is also a challenge for Org Y. They generated a standard suite of security tests for individual teams to run, and provided training on how to perform these. The interviewee felt that "better testing of the requirements greatly helped… [Our] security posture improved as we provided better guidance and examples for test cases." Therefore, they continue to develop better testing tools and provide clear instructions on their use. Monitoring helps ensure sure that tools are used properly at Org Y.

Correction: Correction to Org Y's security program can either come from the executive team or from security architects in the central security team. Both executives and individual contributors were trying to identify gaps in procedures and improve on identified shortcomings. Executives were viewed as less effective in directing correction compared with the security team. The interviewee felt executives "do not take input from individuals on the front line." An executive is responsible for developing new security initiatives, reevaluating goals of the current process, or overseeing projects that would take several years to complete. Lower level security personnel make corrections that tend to focus more tightly on short term efforts and that greatly improve the quality of the existing program.

Comparative Analysis

At both organizations, due care is gauged by the reputations of individuals performing different roles and their perceived trustworthiness. No formal process or specialized training is required to be seen as an authoritative figure in the security programs. Both organizations require that individuals self-certify compliance with internal and external policies, but there was no indication that those individuals were motivated to identify gaps in their own security efforts. Org Y did have a specialized InfoSec training program; however, completion of this program was not necessary for an individual to be authorized to sign-off on compliance efforts. This lack of formal compliance requirements may be because both organizations produce technology products in high velocity markets. In other industries -- such as those that provide services to the government – it is likely more formal care elements are in place.

Communication at Org X was a challenge, while at Org Y a strong security community emerged with dedicated mailing lists and active participation. Org Y executives were sometimes active participants on these mailing lists. At both organizations, interviews did not reveal strong security controls. Controls primarily consisted of tools for testing (identifying) and remediating security issues. While both organizations had policies and procedures for identifying security issues, neither organization collected data on the effectiveness of these policies and procedures. Both companies struggled with consistency and focused on repeatable execution of security testing tools. Both interviewees stressed that improved

training on security tools helped with both consistency and corrective measures (improvements). Similarly, both organizations reported that corrective measures could be initiated by executives (during development of strategic programs) or by individual contributors who made improvements to tools that were being used, in order to provide more accurate information.

Overall, both organizations have well-established and well-respected security programs, but they are not fully developed under the Seven C's model. This would imply that the concept of ethically responsible InfoSec has a strong foundation to support the Seven C's, but its potential has not fully been realized.

Contributions, Limitations, Conclusion

Responsible InfoSec oversight and management is a central requirement for an ethically-responsible organization in a post-industrial world. Findings from our two-case study suggest that the Seven C's provide useful high-level guidance for creating an InfoSec policy and supporting procedures, and overseeing a security culture, by helping leaders identify strengths and potential opportunities for improvement in their organization's InfoSec program. Our two-case study is an important first step in exploring how concepts first proposed in the 1991 Federal Sentencing Guidelines for Organizations can be adapted to suit the context of organizations' InfoSec programs. Our two cases illustrate how specific resources and resource bundles specified by the Seven C's model can contribute to an effective InfoSec program. Our findings show that when complementary technical, structural, or human assets or capabilities are needed but not present, controls may be ineffective. Managers charged with developing, implementing or overseeing InfoSec policies and procedures need to consider how the Seven C's resources can complement one another or prevent the organization from achieving an optimal security posture.

We relied on a single informant for each exploratory case, which is an important study limitation. Stronger case studies rely on interviews at multiple managerial levels, in multiple functions, and triangulating against other internal and external data sources. Also, we chose to study two high-tech companies. A strong long-term program of case research would investigate the applicability of the Seven C's in a variety of companies (such as small versus large or public versus private) in a variety of industries. Studies based on action research (implementing the Seven C's) would also be highly beneficial.

With news of InfoSec breaches increasing in intensity and scope, and with new data protection regulations and breach notification requirements, organizations face intensified scrutiny of the policies and procedures they use to protect information assets and related human and other resources. Much work is needed on many fronts in the Age of Insecurity. We propose that the Seven C's framework can provided useful guidance and we invite others to join us in further evaluating and refining it.

References

Barney, J. 1991. "Firm Resources and Sustained Competitive Advantage," *Journal of Management*, (17:1), pp. 99–120 (doi: 10.1177/014920639101700108).

Beautement, A., Sasse, M. A., and Wonham, M. 2009. "The compliance budget: managing security behaviour in organisations," in *Proceedings of the 2008 workshop on New security paradigms*, ACM, pp. 47–58 (available at http://dl.acm.org/citation.cfm?id=1595684).

Berghout, E., and Tan, C.-W. 2013. "Understanding the impact of business cases on IT investment decisions: An analysis of municipal e-government projects," *Information & Management*, (50:7), pp. 489–506.

Bhatt, G. D., and Grover, V. 2005. "Types of information technology capabilities and their role in competitive advantage: An empirical study," *Journal of management information systems*, (22:2), pp. 253–277.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., and 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), pp. 151–164 (doi: 10.1057/ejis.2009.8).

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Quarterly*, (34:3), pp. 523-A7.

Bureau of Labor Statistics. 2015. "Occupational Outlook Handbook, 2016-17 Edition," Washington DC: U.S. Department of Labor (available at http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-1).

Chen, P., Kataria, G., and Krishnan, R. 2011. "Correlated Failures, Diversification, and Information Security Risk Management," *MIS Quarterly*, (35:2), pp. 397–422.

Collis, D. J., and Montgomery, C. A. 1995. "Competing on Resources: Strategy in the 1990s," *Harvard Business Review*, (73:1), pp. 25–40.
Computer Security Institute. 2011. "2010/2011 CSI Computer Crime and Security Survey," R. Richardson (ed.), New York, NY: Computer Security Institute.
Cremonini, M., and Nizovtsev, D. 2010. "Risks and Benefits of Signaling Information System Characteristics to Strategic Attackers," *Journal of Management Information Systems*, (26:3), p. 241.
Culnan, M. J., and Williams, C. C. 2009. "How Ethics Can Enhance Organizational Privacy: Lessons from the Choicepoint and TJX Data Breaches," *MIS Quarterly*, (33:4), pp. 673–687.
D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research*, (20:1), pp. 79–98.
Denzin, N. K. 2001. *Interpretive interactionism*, Applied Social Research Methods, (Vol. 16), Thousand Oaks, CA: Sage (available at https://books.google.com/books?hl=en&lr=&id=NEpUJLWTWPYC&oi=fnd&pg=PR9&dq=denzin+2001+interpretive+interactionism&ots=xAJcX0FyMT&sig=71LWKMb0D2H30zHC8LjQUAJMDRk).
Dhillon, G., and Torkzadeh, G. 2006. "Value-focused assessment of information system security in organizations," *Information Systems Journal*, (16:3), pp. 293–314 (doi: 10.1111/j.1365-2575.2006.00219.x).
FIRST. 2016a. "Alphabetical list of FIRST Members," January (available at https://www.first.org/members/teams; retrieved March 14, 2016).
FIRST. 2016b. "FIRST History," (available at https://www.first.org/about/history; retrieved March 14, 2016).
Gal-Or, E., and Ghose, A. 2005. "The Economic Incentives for Sharing Security Information," *Information Systems Research*, (16:2), pp. 186–208 (doi: 10.1287/isre.1050.0053).
Goldstein, J., Chernobai, A., and Benaroch, M. 2011. "An Event Study Analysis of the Economic Impact of IT Operational Risk and its Subcategories," *Journal of the Association for Information Systems*, (12:9), pp. 606–631.
Gordon, L. A., Loeb, M. P., and Sohail, T. 2010. "Market Value of Voluntary Disclosures Concerning Information Security," *MIS Quarterly*, (34:3), pp. 567-A2.
Guo, K. H., Yuan, Y., Archer, N. P., and Connelly, C. E. 2011. "Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model," *Journal of Management Information Systems*, (28:2), pp. 203–236.
Hall, J. H., Sarkani, S., and Mazzuchi, T. A. 2011. "Impacts of organizational capabilities in information security," *Information Management & Computer Security*, (19:3), pp. 155–176.
Herath, T., and Rao, H. R. 2009. "Protection motivation and deterrence: a framework for security policy compliance in organisations," *European Journal of Information Systems*, (18:2), pp. 106–125 (doi: 10.1057/ejis.2009.6).
ISACA. 2016. "State of Cybersecurity: Implications for 2016," Rolling Meadows, IL: ISACA, pp. 1–23.
Kaplan, J. M., and Dakin, L. S. 1993. "Living with the Organizational Sentencing Guidelines," *California Management Review*, (36:1), pp. 136–146.
Karahanna, E., Agarwal, R., and Angst, C. M. 2006. "Reconceptualizing compatibility beliefs in technology acceptance research," *Mis Quarterly*, pp. 781–804.
Koch, H., Leidner, D. E., and Gonzalez, E. S. 2013. "Digitally enabling social networks: resolving IT-culture conflict," *Information Systems Journal*, (23:6), pp. 501–523 (doi: 10.1111/isj.12020).
Kwon, J., and Johnson, M. E. 2013. "Health-Care Security Strategies for Data Protection and Regulatory Compliance," *Journal of Management Information Systems*, (30:2), pp. 41–66 (doi: 10.2753/MIS0742-1222300202).
McGahan, A. M., and Porter, M. E. 1997. "How much does industry matter, really?," (available at https://books.google.com/books?hl=en&lr=&id=Pv3wzZ0z7R0C&oi=fnd&pg=PA260&dq=How+much+does+industry+matter+really&ots=E2gF67z5p4&sig=U09VJvOTzGNqmOpAc6OHhx44hA0).
McLaughlin, M.D., D'Arcy, J., Gogan, J., and Cram, W. A. 2017. "Capabilities and Skill Configurations of Information Security Incident Responders," Presented at the Hawaii International Conference on System Sciences, Waikoloa, HI, January.
McLaughlin, M.D., and Gogan, J. 2013. "Complementary Resource Effects Across Organizational Boundaries and the Remediation of Security Incidents.," in *Bled eConference*, Presented at the 26th Bled eConference.
McLaughlin, M.D., and Gogan, J. 2014. "INFOSEC in a Basket, 2004-2013," in *AMCIS*, Presented at the 20th Americas Conference on Information Systems, Savannah, GA.
McLaughlin, M.D., and Gogan, J. 2017. "InfoSec Research in Prominent IS Journals: Findings and Implications for the CIO and Board of Directors," Presented at the Hawaii International Conference on System Sciences, Waikoloa, HI, January.
Miles, M. B., Huberman, A. M., and Saldana, J. 2013. *Qualitative data analysis: A methods sourcebook*, SAGE Publications, Incorporated (available at

https://books.google.com/books?hl=en&lr=&id=3CNrUbTu6CsC&oi=fnd&pg=PR1&dq=fundamentals+of+qualitative+data+analysis&ots=Lg60ohYP7f&sig=aMVfXBcOv0CYK8edaS7aKFfbYjU).

Nowruzi, M., Jazi, H. H., Dehghan, M., Shahmoradi, M., Hashemi, S. H., and Babaeizadeh, M. 2012. "A comprehensive classification of incident handling information," Presented at the Telecommunications (IST), 2012 Sixth International Symposium on, IEEE, pp. 1071–1075.

Penrose, E. T. 1951. *The Theory of the Growth of the Firm*, Wiley (available at https://books.google.com/books?hl=en&lr=&id=aigWHVhP5tsC&oi=fnd&pg=PR22&dq=The+Theory+of+Growth+of+the+Firm.&ots=AVBiOXqhxv&sig=04sD7g51nu1ulOjs-3q4-Pg5-Kk).

Peteraf, M. A. 1993. "The cornerstones of competitive advantage: A resource-based view," *Strategic Management Journal*, (14:3), pp. 179–191.

Ponemon Institute. 2015. "2015 Cost of Cyber Crime Study: United States," Traverse City, Michigan: Ponemon Institute, pp. 1–30.

Powell, T. C. 2001. "Competitive advantage: logical and philosophical considerations," *Strategic management journal*, (22:9), pp. 875–888.

Prahalad, C. K., and Hamel, G. 1990. "The core competence of the corporation," *Harvard Business Review*, (68:3), pp. 79–91.

Prieto, I. M., and Easterby-Smith, M. 2006. "Dynamic capabilities and the role of organizational knowledge: an exploration," *European Journal of Information Systems*, (15:5), pp. 500–510.

Puhakainen, P., and Siponen, M. 2010. "Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study," *MIS Quarterly*, (34:4), pp. 767-A4.

Ray, G., Muhanna, W. A., and Barney, J. B. 2005. "Information technology and the performance of the customer service process: A resource-based analysis," *MIS quarterly*, pp. 625–652.

Safa, N. S., and Von Solms, R. 2016. "An information security knowledge sharing model in organizations," *Computers in Human Behavior*, (57), pp. 442–451.

Siponen, M., and Vance, A. 2010. "Neutralization: New Insights Into the Problem of Employee Information Systems Security Policy Violations," *MIS Quarterly*, (34:3), pp. 487–502.

Stahl, B. C., Doherty, N. F., and Shaw, M. 2012. "Information security policies in the UK healthcare sector: a critical evaluation," *Information Systems Journal*, (22:1), pp. 77–94 (doi: 10.1111/j.1365-2575.2011.00378.x).

Straub, D. W. 1990. "Effective IS security: An empirical study," *Information Systems Research*, (1:3), pp. 255–276.

Teece, D. J. 1986. "Profiting from technological innovation: Implications for integration, collaboration, licensing and public policy," *Research policy*, (15:6), pp. 285–305.

Vance, A., Lowry, P. B., and Eggett, D. 2013. "Using Accountability to Reduce Access Policy Violations in Information Systems," *Journal of Management Information Systems*, (29:4), pp. 263–290 (doi: 10.2753/MIS0742-1222290410).

Vance, A., Lowry, P. B., and Eggett, D. 2015. "Increasing Accountability Through User-Interface Design Artifacts: A New Approach to Addressing the Problem of Access-Policy Violations," *MIS Quarterly*, (39:2).

Wang, T., Kannan, K. N., and Ulmer, J. R. 2013. "The Association Between the Disclosure and the Realization of Information Security Risk Factors," *Information Systems Research*, (24:2), pp. 201-218-495.

Warkentin, M., Johnston, A. C., and Shropshire, J. 2011. "The influence of the informal social learning environment on information privacy policy compliance efficacy and intention," *European Journal of Information Systems*, (20:3), pp. 267–284 (doi: 10.1057/ejis.2010.72).

Weishäupl, E., Yasasin, E., and Schryen, G. 2015. "A Multi-Theoretical Literature Review on Information Security Investments using the Resource-Based View and the Organizational Learning Theory," in *ICIS*, Presented at the ICIS (available at http://aisel.aisnet.org/icis2015/proceedings/SecurityIS/16/).

Wernerfelt, B. 1984. "A resource-based view of the firm," *Strategic Management Journal*, (5:2), pp. 171–180.

West, P., and DeCastro, J. 2001. "The Achilles heel of firm strategy: Resource weaknesses and distinctive inadequacies," *Journal of Management Studies*, (38:3), pp. 417–442.

Yin, R. K. 2009. *Case study research: Design and methods*, (Vol. 5), Sage.

Zietsma, C., Winn, M., Branzei, O., and Vertinsky, I. 2002. "The war of the woods: Facilitators and impediments of organizational learning processes," *British Journal of Management*, (13:S2), pp. S61–S74.