A Design Science Approach to Constructing Critical Infrastructure and Communicating Cybersecurity Risks

Steven Muegge and Dan Craigen

> *"I believe in evidence. I believe in observation, measurement, and reasoning, confirmed by independent observers. I'll believe anything, no matter how wild and ridiculous, if there is evidence for it. The wilder and more ridiculous something is, however, the firmer and more solid the evidence will have to be."*
>
> Issac Asimov (1920–1992)
> Author; In *The Roving Mind*

Academics are increasingly examining the approaches individuals and organizations use to construct critical infrastructure and communicate cybersecurity risks. Recent studies conclude that owners and operators of critical infrastructures, as well as governments, do not disclose reliable information related to cybersecurity risks and that cybersecurity specialists manipulate cognitive limitations to overdramatize and oversimplify cybersecurity risks to critical infrastructures. This article applies a design science perspective to the challenge of securing critical infrastructure by developing a process anchored around evidence-based design principles. The proposed process is expected to enable learning across critical infrastructures, improve the way risks to critical infrastructure are communicated, and improve the quality of the responses to citizens' demands for their governments to collect, validate, and disseminate reliable information on cybersecurity risks to critical infrastructures. These results will be of interest to the general public, vulnerable populations, owners and operators of critical infrastructures, and various levels of governments worldwide.

Introduction

Three problems hinder the construction of critical infrastructure and communication of cybersecurity risks. First, reliable information on the risks of cyber-attacks to critical infrastructures is not readily available. Governments and critical infrastructure owners and operators have placed a veil on reliable information related to cyber-attacks to critical infrastructure (Quigley et al., 2013). Second, cybersecurity specialists who brand themselves as "cyber gurus" manipulate cognitive limitations for the purpose of over-dramatizing and oversimplifying cybersecurity risks to critical infrastructure (Quigley et al., 2015). Third, information sharing across critical infrastructures is constrained by a number of issues, including institutional culture (Baker, 2010; Hood, 1998; Relyea, 2004), and secrecy, competition, and public image (Quigley & Mills, 2014).

Critical infrastructures are those assets or systems that are essential for the maintenance of vital societal functions (Council of the European Commission, 2008). Examples of critical infrastructures include energy and utilities, finance, food, government, information and communication technology, health, water, safety, and manufacturing (Public Safety Canada, 2014).

Each critical infrastructure has areas of relative strength. For example, nuclear power generation excels at planning and regulation, with strong centralized governance that audits and enforces compliance with standards. Telecommunications excels at real-time monitoring and resilience against continuous, voluminous, and ever-changing attacks. Municipal government infrastructures excel at reactive and flexible response – rapidly replying in a measured way as threats are detected. However, despite the evident opportunity for learn-

A Design Science Approach to Constructing Critical Infrastructure and Communicating Cybersecurity Risks

Steven Muegge and Dan Craigen

ing – for each critical infrastructure to learn from the relative strengths of others to improve their own relative weaknesses – there is little evidence that this learning actually occurs in practice. Perhaps more importantly, knowledge production *across* critical infrastructures has thus far been limited. We have growing "knowledge silos" about securing particular infrastructures, but only a small body of knowledge that generalizes across infrastructures. To better protect critical infrastructures against evolving cybersecurity threats, we need more learning between infrastructures and more knowledge production across infrastructures.

Critical infrastructures are "design artifacts" that are created by people. Thus, securing critical infrastructures against cyber-attacks is, at least in part, a design problem. There is a well-developed scholarly literature and a body of practical knowledge about design. By reformulating critical infrastructure protection as a design problem, we offer an alternative perspective that complements the technical, policy, law enforcement, and national defence perspectives that are prevalent in current discourse.

We propose that the design science notion of *design principles* could provide a partial remedy to today's problems by enabling learning between different infrastructures and enabling new knowledge production across infrastructures. Our solution takes the form of a design process anchored around evidence-based design principles for secure critical infrastructures. The proposed process is a "learning machine" in which design principles provide a focal point for collaboration between infrastructures, codify specialized knowledge in a teachable form that can be more easily communicated to others, elevate attention from point solutions to higher-impact problems, enable knowledge sharing between different infrastructures, and increase both the rate of learning and the frequency of opportunities for learning.

The article proceeds as follows. The first section develops a design science perspective on secure critical infrastructures. The second section presents a five-step evidence-based design process anchored around design principles. The next two sections illustrate the systematic application of this "learning machine" process by reviewing the lessons learned from theory and practice, and developing a set of seven evidence-based design principles, respectively. The second-to-last section discusses the contribution, and the final section concludes the article.

A Design Science Perspective

Design can be defined as *the process of inventing objects that perform specific functions* (Baldwin & Clark, 2000). In this definition, inventing is something different from merely selecting between available alternatives: "A problem only calls for design (in the widest sense of that word) when selection cannot be used to solve it" (Alexander, 1964). The notion of "objects" should be interpreted broadly: engineering objects can be designed, but so can organizations, markets, economies, and larger social systems. The serious scholarly study of design originated in the 1960s with early writing and talks by R. Buckminster Fuller (1963), Christopher Alexander (1964), Sydney Gregory (1966), Herbert Simon (1969) and others, and continues to this day.

Simon (1996) defines a *science of design* as "a body of intellectually tough, analytic, partly formalizable, partly empirical, teachable doctrine about the design process" – thus explicitly excluding ideas that are "intellectually soft, intuitive, informal, and cookbooky". Scholars in this domain argue that design science has its own distinct body of knowledge for designing solutions to human problems:

- According to van Aken (2004), design science is distinct from both the *formal sciences,* such as philosophy and mathematics, that build systems of logical propositions, and the *explanatory sciences,* such as physics and sociology, that aim to describe, explain, and predict observable phenomena within a field.

- According to Simon (1996), design science is distinct from both the *natural sciences* and the *social sciences* that try to understand reality.

- Van Aken (2004) further argues that design science is distinct from *applied science,* which more narrowly implies the application of research outcomes from the explanatory sciences.

At least three recurring themes from design science scholarship are salient here:

1. When properly expressed, design knowledge is *teachable.* It can be (partly) captured in an expressive form, and conveyed from one designer to another, or passed down from an experienced senior designer to an apprentice.

A Design Science Approach to Constructing Critical Infrastructure and Communicating Cybersecurity Risks

Steven Muegge and Dan Craigen

2. A subset of design knowledge is connected only with particular problem spaces; other design knowledge is more broadly applicable to categories or families of problem spaces. Consistent with the design science literature, we label the first (more narrow) subset of codified design knowledge as *design rules,* and the second (more broadly applicable) subset of codified design knowledge as *design principles.*

3. It is possible to move between these levels of abstraction – to sometimes "abstract up" from narrow design rules to broader design principles, or to "ground" design principles in the specific context and objective of the problem at hand to formulate solution-oriented and context-specific design rules that lead to specific actions. This mechanics of this process are only partly understood; this continues to be an active area of ongoing research for design science scholars (Denyer et al., 2008; Kauremma, 2009).

These three themes imply that design knowledge – when properly expressed as design principles and design rules – can improve over time through cycles of explanation and experimentation that resemble the theory-building and theory-testing cycles of the scientific method.

Romme and Endenburg (2006) previously proposed a five-step cyclical design process that makes explicit all of these themes and ideas, including the notion of design principles. Although the authors had originally focused on the specific problem of organization design (Dunar & Starbuck, 2006; Jelinek et al., 2008), other researchers have found the process to be both adaptable and extensible. For example, McPhee (2012a) introduced refinements for performance management and for linking design principles to specific actions, and proposed a results-based organization design process for technology entrepreneurs. McPhee (2012b) then employed the process to design the organization that today produces and disseminates the *Technology Innovation Management Review.* Others have adapted the design science process to a diverse range of artifacts; some of the more novel examples include: i) design of policy to foster technology entrepreneurship in a region (Gilsing et al., 2010), ii) heavy construction projects (Voordijk, 2011), iii) corporate ventures (Burg et al., 2012), iv) public participation processes (Bryson et al., 2013), and v) a knowledge management portal (Pascal et al., 2013). Continuing on this path, we adapt the Romme and Endenburg (2006) process and the lessons learned from design science scholarship to the problem of designing secure critical infrastructures.

Process to Construct Critical Infrastructure and Communicate Cybersecurity Risks

A design science process for designing secure critical infrastructures has the following five steps:

1. Gather lessons learned from theory and practice
This step captures "the cumulative body of key concepts, theories, and experientially verified relationships" (Romme & Endenburg, 2006) that are useful for explaining secure critical infrastructures. The source material thus includes the body of knowledge about critical infrastructures and the body of knowledge about cybersecurity. It includes published research on related phenomena – from the natural sciences and engineering of physical systems and software, from the social sciences on human behaviour and the economics of organizations, and from what Craigen (2014) calls the nascent and slowly emerging science of cybersecurity. It also includes practitioner knowledge obtained from people working in field settings. Practitioner knowledge can also be evidence-based (Van de Ven, 2007), but it is more tentative and of uncertain validity – perhaps obtained from a small non-representative sample or even a rare or unique event that is unlikely to repeat, and is necessarily filtered through human experience. Yet, it is essential to the problem at hand, where cybersecurity research is at a very early stage and the current body of knowledge is largely atheoretical (Craigen et al., 2013; Craigen, 2014). Both forms of source material are distilled together into key insights – the "lessons learned" from theory and practice – that are propositional and probabilistic in nature.

2. Formulate design principles
This step develops a coherent set of imperative propositions grounded in the lessons learned from theory and practice. Design principles are *prescriptive* in logical form (van Aken, 2004): "if you want to achieve Y in situation Z, them perform action X". Some prescriptions are *algorithmic* and precise, like a recipe, in a quantitative format that is thoroughly specified. Others are *heuristic,* in the form of a design exemplar, and are partly indeterminate: "if you want to achieve Y in situation Z, then something like action X will help". Design principles are sufficiently general that they could be used by others faced with similar design challenges (McPhee, 2012a). Design knowledge of this form is valuable to practitioners: it is explicit, compact, transferable, actionable, and testable. The *Technology Innovation Management Review* has previously published sets of design propositions about technology startups that globalize early and rapidly (Bailetti, 2012); technology businesses

A Design Science Approach to Constructing Critical Infrastructure and Communicating Cybersecurity Risks

Steven Muegge and Dan Craigen

anchored in platforms, communities, and business ecosystems (Muegge, 2013); and sustainable open source software projects (Schweik, 2013). For our purposes, the objective to be achieved is secure critical infrastructures that are protected from cybersecurity threats; thus, the design principles of interest here should capture the situation-contingent design actions to achieve this result.

3. Formulate design rules
This step produces detailed guidelines that are specific to the design context and are grounded in one or more design principles. "These rules serve as the instrumental bases for design work" (Romme & Endenburg, 2006). Unlike design principles, design rules may be densely interconnected, and are most effective when applied as sets in combination with other design rules. Thus, design rules are tightly bound to the specific circumstances of a particular problem space. For our purposes, the salient circumstances are likely to include the characteristics of the infrastructure, the performance expectations of the provider and other stakeholders, and the ever-changing threat landscape.

4. Design
This step applies the design rules to create a design representation. Components of a design representation could include physical drawings, mathematical models, software representations, specifications using frameworks, narratives, and other formats (Simon, 1996). The outcome is a "blueprint" that can be followed to construct an artifact that implements the design.

5. Implementation and experimentation
This step constructs a design artifact that implements the design. The artifact can tested and modified. Romme and Endenburg (2006) write:

> *"The science-based design cycle is completed, by observing, analyzing, and interpreting the processes and outcomes generated by the design, and where necessary, adapting existing organization theories or building new theory. In addition, experiences and observations regarding implementation and experimentation may lead participants to rethink the design as well as the rules and principles used."*

Behavioural research suggests that expert designers naturally follow a progression from conceptual principles to design action (Newell & Simon, 1972; Simon, 1996), but often do so internally and automatically, without making explicit the lessons learned (step 1) or attending closely to design principles (step 2). Expert designers instead hold these ideas in tacit "mental models" (Peffers et al., 2008) that may be difficult to codify and explain to others (Senge, 1990). The contribution here is making explicit the different activities at each step and the different outputs of each step. Attending deliberately to lessons learned, design principles and design rules can improve performance (Romme & Endenburg, 2008): "If those engaging in a design project develop some awareness of construction principles used, their learning capability as well as the effectiveness of their actions in the project tends to increase". More importantly for the objective of this article, design knowledge is captured in an explicit form that can be explained, shared, challenged, and tested more easily than the tacit design knowledge that is locked up in designer mental models.

The next two sections illustrate the application of the first two steps of this process to propose an initial set of design principles that cross all critical infrastructures.

Step 1: Lessons Learned from Theory and Practice

Step one of the design process requires that we gather insights from theory and practice that will guide our design principles in step two.

The lessons learned about critical infrastructures originated from three types of source material: i) the published literature, ii) discourse with experienced practitioners, and iii) insights from a set of graduate student research projects. All three sources were associated with a graduate course offered in the Technology Innovation Management (TIM; timprogram.ca) program at Carleton University in the Winter term of 2015 (January to April) on the topic of critical infrastructures and cybersecurity. The authors of this article designed and delivered the course.

Lessons from examining the published literature
The first set of insights emerged from a review of the salient literature, including peer-reviewed journal articles, conference papers, government reports and policy documents, publications from providers of critical infrastructures, and articles in national and international newspapers and magazines. We began with a "recommended reading list" of 35 documents about critical infrastructures selected by the authors and provided to students at the beginning of the course. We added approximately 30 additional sources recommen-

A Design Science Approach to Constructing Critical Infrastructure and Communicating Cybersecurity Risks

Steven Muegge and Dan Craigen

ded by graduate students that were discovered during the students' coursework and research projects, and approximately 10 additional sources recommended by guest speakers. Our source material also included the 33 articles about cybersecurity previously published in the *Technology Innovation Management Review* in the July 2013, August 2013, October 2014, November 2014, January 2015, and April 2015 issues on cybersecurity, including the 15 articles reprinted in *Cybersecurity: Best of TIM Review* (Craigen & Gedeon, 2015). We identified seven key insights from the literature and provide examples of sources supporting each insight:

1. Critical infrastructures are of high value to society (Gorman, 2009; Langner, 2011)

2. Critical infrastructures are highly complex and increasingly interconnected (Clemente, 2013; Penderson et al., 2006; Rinaldi et al., 2001)

3. Critical infrastructures differ in important ways from other categories of information systems; for example, critical infrastructure systems may operate for decades with minimal updates (Hurst et al., 2014)

4. Critical infrastructures are constantly under attack – sometimes successfully (Jackson, 2011; Miller & Rowe, 2012)

5. Sophisticated attacks are multifaceted, with multiple stages and components (Langner, 2011; Verizon, 2015)

6. Responses to attacks are not always effective; some analysts blame a shortage of knowledge, skills, and qualified security professionals (CSIS, 2010)

7. Knowledge of cybersecurity is atheoretical (Craigen, 2014; Craigen & Gedeon, 2015; Singh, 2014)

Lessons from discourse with practitioners

The second set of insights emerged from presentations and interactive dialogues with twelve expert guest speakers from six different critical infrastructure sectors: finance, government, mining, nuclear power, policing, and telecommunications. The experts held job titles such as Chief Information Officer (CIO), Chief Strategist, Superintendent, Vice-President, Director, Manager, and Senior Technical Architect. Each expert provided a presentation, followed by questions and interactive discussion with teaching faculty, graduate students, and invited guests, with a total duration ranging from approximately ninety minutes to three hours. The general charter given to experts was to respond to the question “What challenges keep you up at night?" From these dialogues, we identified nine new key insights:

1. In the sectors we examined, cybersecurity is not a competitive differentiator. For example, banks in the Canadian banking industry all offer comparable security; they do not currently compete for customers on the basis of which bank is more secure than its rivals. In the technical language of stakeholder value propositions (Anderson et al., 2006), cybersecurity is most often a point of parity, not a point of difference.

2. There are significant cultural differences between critical infrastructure sectors. For example, the financial sector takes a risk management approach to security, whereas the nuclear industry response is grounded in physical security. In some sectors, cybersecurity is aligned with operational requirements; in other sectors, cybersecurity is not aligned with operational requirements.

3. Critical infrastructures are impacted by massive ongoing changes to cyberspace, including: i) trends towards virtualization, commoditization and open source, ii) the Balkanization of cyberspace, iii) new potential attack vectors (e.g., growth of mobile devices), and iv) shifts in supply chains.

4. Standards compliance is a major challenge from multiple perspectives, including technical, financial, and organizational competency.

5. Experts voiced concerns with a diverse assortment of challenges, including: i) the weakest link being the human (often due to psychological manipulation), ii) trusting a supply chain that has become global in scope, and iii) the inability of cybersecurity defences to keep pace with the wherewithal, agility, entrepreneurship, and bricolage of the adversary.

6. Little is known about adversaries’ capabilities and motivations; a lack of knowledge limits effective response.

7. Experts reinforced the need for better theory and teachable knowledge about cyber-threats.

8. Current approaches to critical infrastructure protection and threat response are insufficient; experts called for enhanced capabilities, more attention to secure design, and a wide set of response mechanisms.

A Design Science Approach to Constructing Critical Infrastructure and Communicating Cybersecurity Risks

Steven Muegge and Dan Craigen

9. Some experts bemoaned the limited adoption of known best practices. Organizations such as the National Institute for Standards and Technology (NIST) in the United States and the Communications Security Establishment (CSE) in Canada, and multinational companies such as Microsoft, publish best practice lists (e.g., CSE, 2014) that, if instituted, could significantly reduce threat exposure. Yet, many organizations have neither the motivation nor the ability to make changes.

Lessons from graduate student assignments

The third set of insights emerged from graduate student course assignments. A total of 41 students formed 16 assignment groups that each delivered three course assignments (one presentation, one document that proposed a solution to management problem, and one document that developed a contribution to theory). Students were expected to examine the documents on the recommended reading list, engage with the expert guest speakers, and perform their own independent reviews of the published literature. The course assignments required significant analysis of published work, as well as synthesis of new results (Alvesson & Sandberg, 2011; Le Pine & Wilcox King, 2010) and evaluation and judgment to develop actionable recommendations and effectively communicate those recommendations to others. Two of the articles in this issue of the *Technology Innovation Management Review* were developed from these assignments (Payette et al., 2015; Tanev et al., 2015), and we expect more publications in the future. The graduate students varied widely in demographics, including a mix of mid-career and early-career work experience, of working professionals and full-time students, and of careers in the security domain and in other areas. From these assignments, we identified five new insights:

1. Accountability for cybersecurity is often unclear. For example, cybersecurity is currently under-addressed in IT service-level agreements (SLAs). When something goes wrong, each group can blame others.

2. The effective assessment and communication of cybersecurity risks should take a "wide lens" perspective on the network, supply chain, and surrounding ecosystem (e.g., Adner, 2012; Muegge, 2013; Tanev et al., 2015). A product-centric focus is inadequate.

3. Maturity models are a promising and under-utilized approach to assessing capabilities and adoption of best practices. These models can take the form of cybersecurity capability maturity models (e.g., Miron & Muita, 2014) or explicitly including cybersecurity in existing capability assessments (e.g., Payette et al., 2015).

4. Theories and frameworks from other domains, such as entrepreneurship, innovation, criminology, economics, and psychology, can provide alternative perspectives on critical infrastructure design and cybersecurity risk. For example, theories of technology adoption could provide perspective on experts' concerns regarding the limited adoption of known best practices.

5. Formal models of IT security are improving (e.g., Craigen et al., 2013; Cybenko, 2014; Hughes & Cybenko, 2013), but more work is needed for critical infrastructures. For example, accurate forecasts of mean-time-to-compromise of long-lived distributed industrial control systems would require new extensions to current models, including new theory and new empirical work.

Step 2: Design Principles for Secure Critical Infrastructures

Step two of the design process requires that we formulate a coherent set of prescriptive and propositional design principles that are anchored in the lessons learned from theory and practice. Each of our seven design principles shares the same desired outcome: a secure critical infrastructure. The seven design principles are as follows:

1. Anchor design activities around cybersecurity design principles

2. Monitor the entire supply chain

3. Assign accountability

4. Know your adversaries

5. Collaborate around common interests

6. Design for resilience

7. Design within a strong culture of cybersecurity

The following subsections elaborate on each design principle.

A Design Science Approach to Constructing Critical Infrastructure and Communicating Cybersecurity Risks

Steven Muegge and Dan Craigen

1. Anchor design activities around cybersecurity design principles

Cybersecurity is largely atheoretical (Craigen, 2014; Craigen & Gedeon, 2015; Singh, 2014), and consequently, our responses to cyber-attacks are, at best, sub-optimal. A design science approach anchored around explicit design principles provides a way of learning from practice. From practice, we make observations and induce propositions, which can lead to predictive and testable theories. From theories, we can deduce principles and rules and thereby better inform providers of critical infrastructure and cybersecurity stakeholders on how to effectively and efficiently design for and respond to cyber-attacks and how to communicate cybersecurity risks.

2. Monitor the entire supply chain

The business enterprises that provide products and services to critical infrastructure providers do not and cannot exist in isolation. Each of these organizations has their own suppliers, customers, and partners, and each of those organizations has its own network of relationships. Supply chains are increasingly global in scope, and highly complex. They increasingly include open source software and other community-developed assets that are not owned or controlled by a traditional supplier. Failure to properly manage the supply chain can result in malicious or poor-quality products being incorporated into a critical infrastructure, with potentially dire consequences. A broader perspective on supply chain risk and managing the entire "innovation ecosystem" is what Adner (2012) calls "seeing with a wide lens" (q.v., Tanev et al., 2015).

3. Assign accountability

Today, many cyberspace warranties are weak with regards to accountability. This weakness can be partly explained by technical limitations, for example, the challenges in measuring and verifying cybersecurity compliance, and partly by risk aversion, avoidance, and transference by stakeholders. Whether by regulation or exercise of customer market power, it is imperative that enterprises, in general, and critical infrastructures, in particular, take ownership of cybersecurity challenges and become accountable for their postures.

4. Know your adversaries

Researchers are learning more about cyber-attacks and cyber-attackers (e.g., Kadivar, 2014; Adegboyega, 2015), including the entities behind prominent attacks, their motivations, their tools and technologies, and the complex innovation ecosystems that produce attacker tools and technologies. Knowledge about adversaries enables designers of critical infrastructures to make better decisions about cybersecurity defences and enables a broader range of responses to threats. Perhaps infrastructure providers can demotivate attackers by removing a political raison d'être or reducing monetization opportunities, or perhaps they can disrupt the attacker's supply chain by attacking the malware market within which the botnet masters and attackers reside.

5. Collaborate around common interests

Cybersecurity is not a challenge faced alone by a critical infrastructure provider. The consequences of compromised security and service interruptions impact individuals, enterprises, economies, and societies. Academia, government, and business each have a role to play, and can invest together around common interests. For example, providers of critical infrastructures can benefit from platforms, community innovations, and participation in business ecosystems in many of the same ways in which entrepreneurs and other organizations benefit (Muegge, 2013). Open source software projects are a high-potential setting for collaboration; critical infrastructure providers tap into the benefits of high-quality software, and other developers and users benefit from the critical infrastructure providers' high demands for security and testing. Design principles can anchor these collaborations and enable learning.

6. Design for resilience

Resilience, broadly speaking, refers to the ability to recover from or adjust easily to misfortune or change (Merriam-Webster, 2015). In the context of information systems, Smith and colleagues (2011) define network resilience as the ability to provide and maintain an acceptable level of service in the face of faults and challenges to normal operation. As the safety community has long understood, single points of failure must be avoided by design. Critical systems must be diverse, resilient, and resistant. Subsystems must be redundant and sandboxed, so that critical infrastructures can tolerate failed or compromised components. Designing for system resilience brings together operational and cybersecurity objectives; protecting critical infrastructures against evolving cybersecurity threats thus becomes an enabler – a necessary condition for achieving operational objectives.

7. Design within a strong culture of cybersecurity

Culture refers here to "a fairly stable set of taken-for-granted assumptions, shared beliefs, meanings, and val-

A Design Science Approach to Constructing Critical Infrastructure and Communicating Cybersecurity Risks

Steven Muegge and Dan Craigen

ues that form a kind of backdrop for action" (Smirchish, 1985). According to Schein (1993), the shared assumptions that are embedded in a strong organizational culture are quickly picked up by new members as "the correct way to perceive, think, and feel". A strong culture of cybersecurity thus refers to an organizational culture in which cybersecurity is deemed normal, where security is expected and valued, and where the negative consequences of compromised security are perceived as abnormal, anomalous, and repugnant, or "not the way things are done around here". For example, groups and individuals would practice safe computing and would expect others to do so. IT systems would be promptly patched, and secure best practices would be the norm. Thus, the seventh design principle brings together the first six design principles and institutionalizes them as "the correct way to perceive, think, and feel."

Contribution

Design science is increasingly applied in the domains of information systems (Hevner et al., 2004; Peffers et al., 2008; Pries-Hehi & Baskerville, 2008) and organization design (Dunbar & Starbuck, 2006; Jelinek et al., 2008; McPhee, 2012b), and a wide array of novel applications including policy design (Gilsing et al., 2010) and process design (Bryson et al., 2013). By developing and applying a design science perspective on secure critical infrastructures, we offer three contributions:

1. We adapt prior work by Romme & Endenburg (2006) to propose a five-step critical infrastructure design process anchored around the creation and application of design principles.

2. We propose a set of seven critical infrastructure design principles that are grounded in theory and evidence.

3. We illustrate the application of the critical infrastructure design process by developing our initial set of seven design principles from the lessons learned from theory and practice. Others can take this process forward to the next steps by formulating context-specific design rules for particular problem spaces by taking into account the target infrastructure and expected threats.

We argue that a design science approach that is anchored in explicit and well-formulated design principles would offer three important benefits:

1. Design principles enable knowledge sharing *between* infrastructures. Design knowledge expressed as design principles is teachable, actionable, and testable.

2. Design principles enable knowledge production *across* infrastructures. Explicit and deliberate attention to design principles elevates the focus of knowledge production and capture from the "sticky" knowledge of domain-specific problems to broader categories of knowledge about critical infrastructures and cybersecurity risks.

3. Design principles can play a central role in the theory-building process. Ideally, design principles would follow from strong theory (Romme & Endenburg, 2006). However, because the current body of knowledge about cybersecurity is largely atheoretical (Craigen et al., 2013; Craigen, 2014), design principles for the foreseeable future are likely to be grounded mainly in practitioner experience rather than strong theory. With a strong set of explicit and well-formulated design principles, researchers could alternate between inductive and deductive cycles of theory-building (Christensen & Raynor, 2003), first generating tentative theoretical explanations that could account for the design principles, then devising empirical tests to distinguish between rival explanations.

Each of the seven initial design principles suggests questions for future research on securing critical infrastructures. First, we need more research on the design process itself, on how to more effectively accomplish each of the steps, and how to transition between steps – for example, on how *specifically* to formulate context-specific design rules that are anchored in a coherent set of design principles. Second, we need a better understanding of how to secure complex global supply chains, and how to estimate, communicate, and manage supply chain risk. Third, we need to better understand accountability for cybersecurity, especially regarding shared and open source assets, and from providers of goods and services for which cybersecurity has not previously been a primary concern. Fourth, we need more information and more timely information about the adversaries of critical infrastructures – their motivations, capabilities, technologies, activities, and business models, and how their operations could be disrupted. Fifth, we need better ways to motivate collective action around shared interests and effectively collaborate. Sixth, we need systems that are more resili-

A Design Science Approach to Constructing Critical Infrastructure and Communicating Cybersecurity Risks

Steven Muegge and Dan Craigen

ent and can continue operating even as specific subsystems fail or are compromised. Seventh, we need cybersecurity to become culturally-embedded in more activities by more stakeholders. As our initial design principles are refined and new design principles are developed and added, we expect the number of interesting and high-impact research questions and problems to grow.

Conclusion

The ongoing success of cyber-attackers and the growing criticism of how cybersecurity risk is communicated is a condemnation of current practice. We confront these problems by developing a design science perspective on secure critical infrastructures, proposing a five-step design process anchored around evidence-based design principles, and demonstrating our "learning machine" approach by gathering lessons learned about critical infrastructures from theory and practice and formulating a set of seven evidence-based design principles.

Our principles are not definitive; rather, they are a starting position to be improved by others. The continued progress of scholarly research, the inclusion of more research results and more practitioner literature, the addition of more experts with field experience in a broader range of infrastructures, and further iteration through the cycles of the design process are all expected to sharpen and refine the starting list of seven principles. We call upon and challenge our readers to apply and extend this work.

About the Authors

Steven Muegge is an Assistant Professor at the Sprott School of Business at Carleton University in Ottawa, Canada, where he teaches and leads a research program within Carleton's Technology Innovation Management (TIM) program. His research, teaching, and community service interests include technology entrepreneurship and commercialization, non-traditional settings for innovation and entrepreneurship (business ecosystems, communities, platforms, and interconnected systems that combine these elements), and business models of technology entrepreneurs (especially in non-traditional settings).

Dan Craigen is a Science Advisor at the Communications Security Establishment in Canada and a Visiting Scholar at the Technology Innovation Management Program of Carleton University in Ottawa, Canada. Previously, he was President of ORA Canada, a company that focused on High Assurance/Formal Methods and distributed its technology to over 60 countries. His research interests include formal methods, the science of cybersecurity, and technology transfer. He was the chair of two NATO research task groups pertaining to validation, verification, and certification of embedded systems and high-assurance technologies. He received his BScH and MSc degrees in Mathematics from Carleton University.

References

Adegboyega, O. 2015. Representing Botnet-Enabled Cyber-Attacks and Botnet Takedowns Using Club Theory. *Technology Innovation Management Review,* 5(6): 35–44. http://timreview.ca/article/905

Adner, R. 2012. *The Wide Lens: A New Strategy for Innovation.* New York, NY: Portfolio/Penguin.

Alexander, C. 1964. *Notes on the Synthesis of Form.* Cambridge, MA: Harvard University Press.

Alvesson, M., & Sandberg, J. 2011. Generating Research Questions through Problematization. *Academy of Management Review,* 36(2): 247–271.

Anderson, J. C., Narus, J. A. & van Rossum, W. 2006. Customer Value Propositions in Business Markets. *Harvard Business Review,* 84(3): 90–99.

Bailetti, T. 2012. What Technology Startups Must Get Right to Globalize Early and Rapidly. *Technology Innovation Management Review,* 2(10): 5–16. http://timreview.ca/article/614

Baker, S. 2010. *Skating on Stilts: Why We Aren't Stopping Tomorrow's Terrorism.* Hoover Institution Press Publication no. 591. Stanford, CA: Hoover Institution at Leland Stanford Junior University.

Baldwin, C. Y., & Clark, K. B. 2000. *Design Rules: Volume 1: The Power of Modularity.* Cambridge, MA: MIT Press.

Burg, E., Jager, S., Reymen, I. J., & Cloodt, M. 2012. Design Principles for Corporate Venture Transition Processes in Established Technology Firms. *R&D Management,* 42(5): 455–472. http://dx.doi.org/10.1111/j.1467-9310.2012.00695.x

Bryson, J. M., Quick, K. S., Slotterback, C. S., & Crosby, B. C. 2013. Designing Public Participation Processes. *Public Administration Review,* 73(1): 23–34. http://dx.doi.org/10.1111/j.1540-6210.2012.02678.x

A Design Science Approach to Constructing Critical Infrastructure and Communicating Cybersecurity Risks

Steven Muegge and Dan Craigen

Center for Strategic & International Studies (CSIS). 2013. *A Human Capital Crisis in Cybersecurity: Technical Proficiency Matters.* Washington, DC: Center for Strategic and International Studies.

Christensen, C. M., & Raynor, M. E. 2003. Why Hard-Nosed Executives Should Care about Management Theory. *Harvard Business Review,* 81(9): 66–74.

Clemente, D. 2013. *Cybersecurity and Global Interdependence: What is Critical?* London, UK: Chathamhouse.

Communication Security Establishment (CSE). 2014. *Top 10 Security Actions to Protect Government of Canada Internet-Connected Networks and Information Systems.* IT Security Bulletin of the Government of Canada, ITSB-89 Version 3.

Council of the European Union. 2008. Council Directive 20008/114/EC on the Identification and Designation or European Critical Infrastructures and the Assessment of the Need to Improve Their Protection. *Official Journal of the European Union,* L 345: 75–82.

Craigen, D. 2014. Assessing Scientific Contributions: A Proposed Framework and Its Application to Cybersecurity. *Technology Innovation Management Review,* 4(11): 5–13. http://timreview.ca/article/844

Craigen, D., & Gedeon, I. (Eds.). 2015. *Cybersecurity: Best of TIM Review.* Ottawa, Canada: Talent First Network.

Craigen, D., Walsh, D. A., & Whyte, D. 2013. Securing Canada's Information-Technology Infrastructure: Context, Principles, and Focus Areas of Cybersecurity Research. *Technology Innovation Management Review,* 3(7): 12–18. http://timreview.ca/article/704

Cybenko, G. 2014. TIM Lecture Series – Cybersecurity Metrics and Simulation. *Technology Innovation Management Review,* 4(10): 43–45. http//timreview.ca/article/839

Denyer, D., Tranfield, D,. van Aken, J. E. 2008. Developing Design Propositions through Research Synthesis. *Organization Studies,* 29(3): 393–413. http://dx.doi.org/10.1177/0170840607088020

Dunbar, R. L. M., & Starbuck, W. H. 2006. Learning to Design Organizations and Learning from Them. *Organization Science,* 17(2): 171–178. http://dx.doi.org/10.1287/orsc.1060.0181

Fuller, R. B. 1963. World Design Initiative: Discourse to the 'International Symposium on Architecture' of the Union of International Architects. In R. B. Fuller (Ed.), *Inventory of World Resources: Phase 1 Document 2: The Design Initiative:* 1–104. Carbondale, IL: Southern Illinois University.

Gregory, S. 1966. *The Design Method.* New York: Plenum Press.

Gilsing, V. A., van Burg, E., & Romme, A. G. L. 2010. Policy Principles for the Creation and Success of Corporate and Academic Spin-Offson to Cybersecurity. *Technovation,* 30(1): 12–23. http://dx.doi.org/10.1016/j.technovation.2009.07.004

Gorman, S. 2009. Electricity Grid in U.S. Penetrated By Spies. *The Wall Street Journal,* April 8, 2009. Accessed June 1, 2015: http://www.wsj.com/articles/SB123914805204099085

Hevner, A. R., March, S. T., Park, J. & Ram, S. 2004. Design Science in Information Systems Research. *MIS Quarterly,* 28(1): 75–105.

Hood, C. 1998. *The Art of the State: Culture, Rhetoric and Public Management.* Oxford: Oxford University Press.

Hughes, J., & Cybenko, G. 2013. Quantitative Metrics and Risk Assessment: The Three Tenets Model of Cybersecurity. *Technology Innovation Management Review,* 3(8): 15–24. http://timreview.ca/article/712

Hurst, W., Merabti, M., & Fergus, P. 2014. A Survey of Critical Infrastructure Security. *IFIP Advances in Information and Communication Technology,* 411: 127–138. http://dx.doi.org/10.1007/978-3-662-45355-1_9

Jackson, W. 2011. After 13 Years, Critical Infrastructure Security Still Lacking. *GCN,* July 27, 2011. Accessed June 1, 2015: http://gcn.com/articles/2011/07/27/critical-infrastructure-still-vulnerable-house-hearing.aspx

Jelinek, M., Romme, A. G. L., & Boland, R. J. 2008. Organization Studies as a Science for Design: Creating Collaborative Artifacts and Research. *Organization Studies,* 29(3): 317–329. http://dx.doi.org/10.1177/0170840607088016

Kadivar, M. 2014. Cyber-Attack Attributes. *Technology Innovation Management Review,* 4(11): 22–27. http://timreview.ca/article/846

Kauremaa, J. 2009. *Committed to Field Problems: Design Science within Management Studies. A Panel Discussion between Joan Ernst Van Aken, Mikko Ketokivi, and Jan Holmstron, October 1 2009.* Espoo, Finland: Aalto University. http://legacy-tuta.hut.fi/logistics/publications/Design-Science-Conversation_20091001_FINAL.pdf

Langner, R. 2011. Stuxnet: Dissecting a Cyberwarfare Weapon. I*EEE Security & Privacy,* 9(3): 48–51. http://dx.doi.org/10.1109/MSP.2011.67

LePine, J. A., & Wilcox King, A. 2010. Editors' Comments: Developing Novel Theoretical Insight from Reviews of Existing Theory and Research. *Academy of Management Review,* 35(4): 508–509.

McPhee, C., 2012a. Results-Based Organization Design for Technology Entrepreneurs. *Technology Innovation Management Review,* 2(5): 10–17. http://timreview.ca/article/554

McPhee, C. 2012b. *Using a Results-Based Organization Design Methodology to Construct the* Technology Innovation Management Review. MASc Thesis. Ottawa, Canada: Carleton University. https://curve.carleton.ca/theses/28419

Merriam-Webster. 2015. *Merriam-Webster's Collegiate Dictionary* (11th ed.). Springfield, MA: Merriam-Webster.

Miller, B., & Rowe, D. C. 2012. A Survey of SCADA and Critical Infrastructure Incidents. In *Proceedings of the 1st Annual Conference on Research in Information Technology (RIIT 2012):* 51–56. http://dx.doi.org/10.1145/2380790.2380805

Miron, W., & Muita, K. 2014. Cybersecurity Capability Maturity Models for Providers of Critical Infrastructure. *Technology Innovation Management Review,* 4(10): 33–39. http://timreview.ca/article/837

Muegge, S. 2013. Platforms, Communities, and Business Ecosystems: Lessons Learned about Technology Entrepreneurship in an Interconnected World. *Technology Innovation Management Review,* 3(2): 5–15. http://timreview.ca/article/655

Newell, A. & Simon, H. A. 1972. *Human Problem Solving.* Englewood Cliffs, NJ: Prentice Hall.

A Design Science Approach to Constructing Critical Infrastructure and Communicating Cybersecurity Risks

Steven Muegge and Dan Craigen

Pascal, A., Thomas, C., & Romme, A. G. L. 2013. Developing a Human-Centred and Science-Based Approach to Design: The Knowledge Management Platform Project. *British Journal of Management,* 24(2): 264–280. http://dx.doi.org/10.1111/j.1467-8551.2011.00802.x

Payette, J., Anegbe, A., Caceras, E., & Muegge, S. 2015. Secure By Design: Cybersecurity Extensions to Project Management Maturity Models for Critical Infrastructure Projects. *Technology Innovation Management Review,* 5(6): 26–34. http://timreview.ca/article/904

Peffers, K., Tuunanen, T., Rothenberger, M. A., and Chatterjee, S. 2008. A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems,* 24(3): 45–77. http://dx.doi.org/10.2753/MIS0742-1222240302

Penderson, P., Dudenhoeffer, D., Hartley, S., & Permann, M. 2006. *Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research.* Idaho Falls, ID: Idaho National Laboratory.

Pries-Heje, J. & Baskerville, R. 2008. The Design Theory Nexus. *MIS Quarterly,* 32(4): 731–755. http://www.jstor.org/stable/25148870

Public Safety Canada. 2014. *National Strategy for Critical Infrastructure.* Ottawa, Canada: Government of Canada.

Quigley, K., Burns, C., & Stallard, K. 2013. *Communicating Effectively about Cyber-Security Risks: Probabilities, Peer Networks and a Longer Term Education Program.* Halifax, Canada: Dalhousie University.

Quigley, K., & Mills, B. 2014. C*ontextual Issues That Influence the Risk Regulation Regime of the Transportation Sector.* Halifax, Canada: Dalhousie University.

Quigley, K., Burns, C., & Stallard, K. 2015. 'Cyber Gurus': A Rhetorical Analysis of the Language of Cybersecurity Specialists and the Implications for Security Policy and Critical Infrastructure Protection. *Government Information Quarterly,* 32(2): 108–117. http://dx.doi.org/10.1016/j.giq.2015.02.001

Relyea, H.C. 2004. Homeland Security and Information Sharing: Federal Policy Considerations. *Government Information Quarterly,* 21(4): 420–438. http://dx.doi.org/10.1016/j.giq.2004.08.007

Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. 2001. Critical Infrastructure Interdependencies. *IEEE Control Systems Magazine,* 21(6): 11–25. http://dx.doi.org/10.1109/37.969131

Romme, A. G. L., & Endenburg, G. 2006. Construction Principles and Design Rules in the Case of Circular Design. *Organization Science,* 17(2): 287–297. http://dx.doi.org/10.1287/orsc.1050.0169

Schein, E. H. 1993. *Organizational Culture and Leadership* (2nd ed.). San Francisco: Jossey-Bass.

Schweik, C. M. 2013. Sustainability in Open Source Software Commons: Lessons Learned from an Empirical Study of SourceForge Projects. *Technology Innovation Management Review,* 3(1): 13–19. http://timreview.ca/article/645

Senge, P. M. 1990. *The Fifth Discipine: The Art and Practice of the Learning Organization.* New York: Doubleday/Currency.

Simon, H. A. 1969. *The Sciences of the Artificial.* Cambridge, MA: MIT Press.

Simon, H. A. 1996. *The Sciences of the Artificial* (3rd ed.). Cambridge, MA: MIT Press.

Singh, M. P. 2013. Toward a Science of Cybersecurity. *Computing Now,* January 2013. Accessed June 1, 2015: http://www.computer.org/web/computingnow/archive/january2013

Smircich, L. 1983. Concepts of Culture and Organizational Analysis. *Administrative Science Quarterly,* 28(3): 339–358. http://www.jstor.org/stable/2392246

Smith, P., Hutchison, D, Sterbenz, J. P. G., Scholler, M., Fessi, A., Karaliopoulos, M., Lac, C., & Plattner, B. 2011. Network Resilience: A Systematic Approach. *IEEE Communications Magazine,* 49(7): 88–97. http://dx.doi.org/10.1109/MCOM.2011.5936160

Tanev, G., Tzolov, P., & Apiafi, R. 2015. A Value Blueprint Approach to Cybersecurity in Networked Medical Devices. *Technology Innovation Management Review,* 5(6): 17–25. http://timreview.ca/article/903

van Aken, J. E. 2004. Management Research Based on the Paradigm of the Design Sciences: The Quest for Field-Tested and Grounded Technological Rules. *Journal of Management Studies,* 41(2): 219–246. http://dx.doi.org/10.1111/j.1467-6486.2004.00430.x

Van de Ven, A. H. 2007. *Engaged Scholarship: A Guide for Organizational and Social Research.* New York, NY: Oxford University Press.

Verizon. 2015. *2015 Data Breach Investigations Report.* New York, NY: Verizon Communications Inc.

Voordijk, H. 2011. Construction Management Research at the Interface of Design and Explanatory Science. *Engineering Construction & Architectural Management,* 18(4): 334–342. http://dx.doi.org/10.1108/09699981111145790

Citation: Muegge, S., & Craigen, D. 2015. A Design Science Approach to Constructing Critical Infrastructure and Communicating Cybersecurity Risks. *Technology Innovation Management Review,* 5(6): 6–16. http://timreview.ca/article/902

Keywords: critical infrastructures, cybersecurity, design science, design propositions, resilience, advanced persistent threats