Technology Innovation Management Review

June 2015
Volume 5 Issue 6

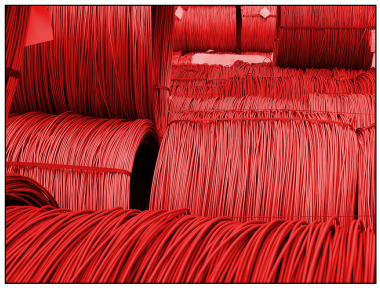

Image licensed under CC BY by Erich Ferdinand

Critical Infrastructures and Cybersecurity

Welcome to the June 2015 issue of the *Technology Innovation Management Review*. This month's editorial theme is Critical Infrastructures and Cybersecurity. We welcome your comments on the articles in this issue as well as suggestions for future article topics and issue themes.

Carleton UNIVERSITY

www.timreview.ca

Technology Innovation Management Review

June 2015
Volume 5 Issue 6

Publisher

The *Technology Innovation Management Review* is a monthly publication of the Talent First Network.

ISSN

1927-0321

www.timreview.ca

Overview

The *Technology Innovation Management Review* (TIM Review) provides insights about the issues and emerging trends relevant to launching and growing technology businesses. The TIM Review focuses on the theories, strategies, and tools that help small and large technology companies succeed.

Our readers are looking for practical ideas they can apply within their own organizations. The TIM Review brings together diverse viewpoints – from academics, entrepreneurs, companies of all sizes, the public sector, the community sector, and others – to bridge the gap between theory and practice. In particular, we focus on the topics of technology and global entrepreneurship in small and large companies.

We welcome input from readers into upcoming themes. Please visit timreview.ca to suggest themes and nominate authors and guest editors.

Contribute

Contribute to the TIM Review in the following ways:

- Read and comment on articles.
- Review the upcoming themes and tell us what topics you would like to see covered.
- Write an article for a future issue; see the author guidelines and editorial process for details.
- Recommend colleagues as authors or guest editors.
- Give feedback on the website or any other aspect of this publication.
- Sponsor or advertise in the TIM Review.
- Tell a friend or colleague about the TIM Review.

Please contact the Editor if you have any questions or comments: timreview.ca/contact

About TIM

The TIM Review has international contributors and readers, and it is published in association with the Technology Innovation Management program (TIM; timprogram.ca), an international graduate program at Carleton University in Ottawa, Canada.

Editorial: Critical Infrastructures and Cybersecurity

Chris McPhee, Editor-in-Chief

Dan Craigen and Steven Muegge, Guest Editors

From the Editor-in-Chief

Welcome to the June 2015 issue of the *Technology Innovation Management Review*. The editorial theme of this issue is **Critical Infrastructures and Cybersecurity**, and I am pleased to welcome our guest editors, **Dan Craigen**, Science Advisor at Communications Security Establishment Canada, and **Steven Muegge**, Assistant Professor in the Sprott School of Business at Carleton University in Ottawa, Canada.

In July, we welcome professors **Patrick Cohendet** and **Laurent Simon** from HEC Montréal as guest editors for a special issue on the theme of **Creativity in Innovation**.

For our August and September issues, we are accepting general submissions of articles on technology entrepreneurship, innovation management, and other topics relevant to launching and growing technology companies and solving practical problems in emerging domains. Please contact us (timreview.ca/contact) with potential article topics and submissions.

We hope you enjoy this issue of the TIM Review and will share your comments online.

Chris McPhee
Editor-in-Chief

From the Guest Editors

It is our pleasure to be guest editors for the June 2015 issue of the TIM Review on **Critical Infrastructures and Cybersecurity**. This is the seventh issue of the TIM Review on the theme of cybersecurity, but it is the first to focus specifically on critical infrastructures – the assets essential for the functioning of a modern society. Along with the publication last month of *Cybersecurity: Best of TIM Review*, the fourth and newest title in the "Best of TIM Review" book series, this issue contributes to the growing body of work on cybersecurity advanced by the TIM Review.

This issue comprises four research articles and a report on a recent TIM lecture. All five articles share a connection with Carleton University in Ottawa, Canada, and Carleton's Technology Innovation Management (TIM; timprogram.ca) program. The first three articles arose from a TIM "Advanced Topics" graduate course on critical infrastructures and cybersecurity that included twelve expert guest speakers from six different critical infrastructure sectors speaking about "What challenges keep you up at night?" The fourth article presents research results obtained from a Master of Applied Science thesis at Carleton. The fifth article reports on a Carleton cybersecurity event.

The guest editors, **Steven Muegge**, an Assistant Professor at the Sprott School of Business at Carleton University, and **Dan Craigen**, a Science Advisor at the Communications Security Establishment and a Visiting Scholar at the Carleton's Technology Innovation Management program, contribute a design science perspective on constructing critical infrastructures. The article introduces a five-step "learning machine" design process anchored around evidence-based design principles, proposes an initial set of seven critical infrastructure design principles that are grounded in theory and evidence, and illustrates the application of the process by developing the design principles from lessons learned from theory and practice. The pro-

Editorial: Critical Infrastructures and Cybersecurity

Chris McPhee, Dan Craigen, and Steve Muegge

posed process will enable knowledge sharing between infrastructures, new knowledge production across infrastructures, and the creation and testing of better theories of cybersecurity.

George Tanev, **Peyo Tzolov**, and **Rollins Apiafi**, three Master of Applied Science candidates in the Technology Innovation Management program, examine the healthcare infrastructure and the cybersecurity of networked medical devices. The article proposes an ecosystem approach to identify and address cybersecurity risks, and demonstrates the approach on a networked insulin pump and continuous glucose monitor. Product vendors can employ this approach to include cybersecurity as a value proposition to customers and as a point of difference from competitors.

Jay Payette, a graduate student in Carleton's Master of Design program, with **Esther Anegbe** and **Erika Caceres**, graduate students in the Technology Innovation Management program, and **Steven Muegge**, a professor in the TIM program, examine the problem of securing the information technology (IT) projects deployed within critical infrastructures. The article proposes a set of cybersecurity extensions to the PjM3, a popular project management maturity model. IT project managers and critical infrastructure providers can employ these extensions to securely "design in" cybersecurity to new IT systems.

Olukayode Adegboyega, a recent graduate of the TIM program, examines the growing problem of botnets and the take-down initiatives that can disrupt botnet networks. The article examines five scenarios of botnet-enabled cyber-attacks and five scenarios of botnet take-downs, and employs club theory to develop new representations of these phenomena. Critical infrastructure providers and other organizations could employ these results to more effectively prepare for and respond to botnet attacks.

The issue concludes with a report on the May 2015 TIM Lecture Series event titled "Three Collaborations Enabling Cybersecurity". **Deborah Frincke**, the Director of Research for the National Security/Central Security Service in the United States, provided the keynote address. **Dan Craigen** announced the official release of the new ebook, *Cybersecurity: The Best of TIM Review* (amazon.com/dp/B00XD3O6L0), co-edited with **Ibrahim Gedeon**, Chief Technology Officer of TELUS. Finally, three speakers from companies belonging to the Lead To Win Cybersecurity Hub – **Ned Nadima** of Denilson, **Arthur Low** of Crack Semiconductor, and **Michael Thomas** of Bedarra Research Labs – provided presentations about their companies' approaches to confronting challenging cybersecurity problems.

We hope that our readers enjoy this month's issue on Critical Infrastructures and Cybersecurity, and come away with practical ideas to apply within their own organizations.

Dan Craigen and Steven Muegge
Guest Editors

Editorial: Critical Infrastructures and Cybersecurity

Chris McPhee, Dan Craigen, and Steve Muegge

About the Editors

Chris McPhee is Editor-in-Chief of the *Technology Innovation Management Review*. He holds an MASc degree in Technology Innovation Management from Carleton University in Ottawa, Canada, and BScH and MSc degrees in Biology from Queen's University in Kingston, Canada. Chris has over 15 years of management, design, and content-development experience in Canada and Scotland, primarily in the science, health, and education sectors. As an advisor and editor, he helps entrepreneurs, executives, and researchers develop and express their ideas.

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.

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).

Citation: McPhee, C., Craigen, D., & Muegge, S. 2014. Editorial: Critical Infrastructures and Cybersecurity. *Technology Innovation Management Review*, 5(6) 3–5. http://timreview.ca/article/901
Keywords: cybersecurity, critical infrastructure, design science, design principles, healthcare, networked medical devices, project management maturity model, botnet, club theory

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

A Value Blueprint Approach to Cybersecurity in Networked Medical Devices

George Tanev, Peyo Tzolov, and Rollins Apiafi

> *"When the value proposition requires multiple elements to converge, you need an approach that will allow you to assess alternative configurations and generate shared understanding and agreement among the partners as to how these elements should come together. … Left unarticulated, contradicting visions don't conflict until after commitments are made and pieces are brought together. But when the strategy meets reality, details become disasters."*
>
> Ron Adner
> Professor of Strategy and Entrepreneurship
> In *The Wide Lens*

Cybersecurity for networked medical devices has been usually "bolted on" by manufacturers at the end of the design cycle, rather than integrated as a key factor of the product development and value creation process. The recently released cybersecurity guidelines by the United States Food and Drug Administration (FDA) offer an opportunity for manufacturers to find a way of positioning cybersecurity as part of front-end design, value creation, and market differentiation. However, the technological architecture and the functionality of such devices require an ecosystem approach to the value creation process. Thus, the present article adopts an ecosystem approach to including cybersecurity as part of their value proposition. It extends the value blueprint approach suggested by Ron Adner to include an additional dimension that offers the opportunity to define: the potential locations of cybersecurity issues within the ecosystem, the specific nature of these issues, the players that should be responsible for addressing them, as well as a way to articulate the added cybersecurity value as a competitive differentiator to potential customers. The value of the additional blueprint dimension is demonstrated through a case study of a representative networked medical device – a connected insulin pump and continuous glucose monitor.

Introduction

Concerns over the state of medical device cybersecurity have become a topic of intense public discussion after cases such as the hacking of connected insulin pumps by researchers to deliberately deliver lethal insulin doses (Healey et al., 2015). Following these cases and similar others, the United States Department of Homeland Security began investigating two dozen medical devices for potential security vulnerabilities and the Food and Drug Administration released guidance to manufacturers for establishing cybersecurity management strategies for their medical devices (FDA, 2014). Experts have come forward stating that the medical device industry is significantly behind other industries in terms of its ability to both articulate and address cybersecurity issues (Fu & Blum, 2014). Also, with networked medical devices increasingly joining the Internet of Things, security will take a much more prominent role as risks to patient health, safety, and data privacy continue to grow (Wirth, 2011). Between 2013 and 2014, the increase in information security breaches for healthcare facilities was almost double that of other industries (Harries, 2014), and with networked devices moving from hospital networks to home networks, new threats are bound to emerge. With public and regulatory pressure rising, manufacturers are spending more time, effort, and resources on im-

A Value Blueprint Approach to Cybersecurity in Networked Medical Devices

George Tanev, Peyo Tzolov, and Rollins Apiafi

proving cybersecurity. At the same time, the existing ways of articulating customer value in the medical device industry do not seem to allow for a differentiation in terms of cybersecurity benefits. These growing cybersecurity concerns and the lack of cybersecurity benefit-articulation highlight the growing need for manufacturers to begin utilizing security as a market value and differentiator.

One of the main criticisms of medical device cybersecurity is that security tends to be added on at the end of the development process, instead of being "baked in" from the start as part of the design phase (Shah, 2015). This late consideration highlights a key problem in the way many manufacturers approach security. Security is perceived as a hurdle to jump over, rather than a key part of the value proposition that can be used as a market differentiator. With an estimated unit sale of networked medical devices to increase by five times from 2012 to 2018 (Healey et al., 2015), increased security efforts are becoming a necessity. These additional efforts provide an opportunity for manufacturers to add value and differentiate themselves in such a growingly competitive market.

Networked medical device are predominately software-based medical devices that are connected to networks involving patients, healthcare organizations, medical specialists, and other service providers. In most of the cases, their operation requires wireless connectivity and multiple interoperations including the sharing of clinical information and controlling other medical devices and systems as well as nonmedical equipment (e.g., routers and servers) and software. Complex networked systems, including medical devices, have now become common, and with this added sophistication, new behaviours and unexpected consequences have begun to appear that are outside the control of the medical device manufacturer (Rakitin, 2009). A report by the Atlantic Council assessing the benefits and risks of healthcare systems in the Internet of Things identifies four main types of networked medical devices (Healey et al., 2015):

1. Embedded devices (e.g., pacemakers)

2. External devices (e.g., insulin pumps)

3. Stationary devices (e.g., networked infusion pumps)

4. Consumer products for health monitoring (e.g., FitBit or Nike Fuel band)

Consumer products for health monitoring are sometimes not discussed with medical devices because they do not require regulatory approval (i.e., they do not fit the definition of a medical device in most regions), but the regulatory framework around them has been under intensive discussion and is likely to change in the coming years (Healey et al., 2015). We will therefore include them as part of our discussion. The rest of the article is organized as follows. We will next describe the specifics of cybersecurity issues in the medical device sector. Then, we will summarize the key points of the value blueprint approach (Adner, 2012) and suggest an additional dimension that addresses cybersecurity issues. The next section contains an application of the cybersecurity blueprinting approach to a specific case consisting of a connected insulin pump and continuous glucose monitor. Finally, we conclude by articulating the key contributions of the article and offering suggestions for future research.

Cybersecurity for Medical Devices

Cybersecurity for medical devices has traditionally been seen as a tradeoff to usability, and therefore as a potential challenge for market value. Even the FDA emphasizes that improved security should be counter-balanced against reduced usability (FDA, 2014). This tradeoff is true in certain cases, but an overemphasis would lead to missing the opportunity to articulate security as add-on value. For example, securing an insulin pump with a password for daily tasks is cumbersome and patients will most likely use a simple password or find a way around it. In another example, encrypting wireless communication of a pacemaker would improve security while also adding value to the patients because they would be safe from malicious threats. With the medical device market already being highly competitive, not articulating security improvements as an add-on value to the patient is a missed opportunity.

In order to articulate the created cybersecurity value, manufacturers of networked medical devices must first change the way they look at the security landscape. Networked medical devices should be seen as a platform in a diverse ecosystem of stakeholders (Shah, 2015), which is similar to mobile communication platforms in the automotive industry. The ecosystem depends on numerous software and hardware systems, some of which have been developed by suppliers and must be integrated using “glue code” so that they can function together (Amin et al., 2015). The integration increases the

A Value Blueprint Approach to Cybersecurity in Networked Medical Devices

George Tanev, Peyo Tzolov, and Rollins Apiafi

chances of introducing cybersecurity vulnerabilities at the interfaces between the different software and electronics systems. The glue code problem can be framed as a knowledge coordination problem between manufacturers and suppliers of networked medical devices. For example, a portable heart monitor communicates to a mobile device, which displays relevant health data and also uploads it to a server for additional post-processing and analytics. Thus, vulnerabilities could be at another location in the ecosystem and not in the device itself, which requires a high degree of knowledge coordination between manufacturers, suppliers, co-innovators, and adoption chain partners. To highlight security as part of the value proposition, we must move from a product-centric approach to an ecosystem-driven approach to security. This approach would allow manufacturers to:

1. *Identify key stakeholders* in the ecosystem together with all associated cybersecurity vulnerabilities.

2. *Create a plan* to address the highest risk cybersecurity vulnerabilities in collaboration with stakeholders.

3. *Articulate the value dimensions* associated with the security efforts to the relevant stakeholders.

4. *Improve security* by innovating the ecosystem.

This article aims to address these points by adapting a value blueprint approach to cybersecurity.

A Value Blueprint Approach to Cybersecurity

The value blueprint approach proposed by Ron Adner in his book *The Wide Lens* (Adner, 2012) takes an ecosystem approach to value creation. Translating a specific value proposition into a value blueprint makes it possible to identify and visualize the multiple dependencies within the ecosystem as well as deal with situations where multiple elements need to converge and a shared understanding between stakeholders is required. Adner suggests an approach to value blueprint development including the following steps:

1. Identify your end customer.

2. Identify your own project.

3. Identify your suppliers.

4. Identify your intermediaries.

5. Identify your complementors.

6. Identify the risks in your ecosystem (Red=Unmitigable risk; Yellow=Mitigable risk; Green=Acceptable risk):
    a. Level of co-innovation risk
    b. Level of adoption risk

7. For every partner whose status is not green, understand the problem and suggest a viable solution.

8. Update blueprint on a regular basis.

The risk levels in Adner's blueprint follow a green, yellow and red "traffic light" approach. It focuses solely on the interplay between co-innovation and adoption chain risks in managing value creation and articulating the market value of the product. For co-innovation risk, green means that the stakeholder is ready and in place, yellow means that they are in place, but do there is no plan, and red means that they are not in place. For adoption risk, green means that partners are eager to participate and see the benefit of their involvement, yellow means that partners are neutral but open to involvement, and red means that they prefer the status quo and are not willing to be involved. A red light would indicate that more substantial changes need to be made in the blueprint, such as a change in partners.

The blueprint could be used however to analyze an additional dimensions of value, and in particular, the value of cybersecurity in networked medical devices. In this way, a blueprint would allow for an explicit analysis of security vulnerabilities from an ecosystem perspective. It would also allow for using all value blueprint tools focusing on evolving the ecosystem to enhance the security of networked medical devices, as well as for articulating the newly created cybersecurity value for a better market differentiation.

The cybersecurity blueprint can be generated by the process proposed by Adner, with minor changes in the way of approaching risks in the ecosystem. For the sake of simplicity, we will assume that all other aspects of value for all stakeholders have been already articulated, and that the risk we are assessing in our value blueprint is strictly cybersecurity risk. This assumption requires some changes to Adner's steps, mostly after step 5. The steps for developing the cybersecurity blueprint for a networked medical device are as follows:

A Value Blueprint Approach to Cybersecurity in Networked Medical Devices

George Tanev, Peyo Tzolov, and Rollins Apiafi

1. Identifying your end customer, your own project, your suppliers, your intermediaries, complementors together with their specific cybersecurity concerns, if any (steps 1–5 in Adner's approach).

2. Identify the locations of security risks in your ecosystem by taking into account any concerns that were explicitly articulated by the different stakeholders (Red=Unmitigable risk; Yellow=Mitigable risk; Green=Acceptable risk).

3. For every location in the blueprint understand the co-innovation (i.e., technical) and adoption aspects of the problems and prioritize them by using an appropriate cybersecurity risk-analysis framework into green (acceptable), yellow (mitigable), and red (unmitigable) risks levels.

4. Develop a risk management action plan to address the highest priority risks (yellow and red) with a viable security risk mitigation measure to make the risk level acceptable (green) and add it to the blueprint as appropriate.

5. Use the cybersecurity blueprint to articulate the value created by your efforts and the next steps in your cybersecurity management plan in a way that you could differentiate in the marketplace.

6. Update and innovate the cybersecurity blueprint on a regular basis.

The changes would allow for the localization of cybersecurity risks within the ecosystem, subsequently taking adequate action to mitigate the risk, and using the blueprint to articulate the security efforts and the value added. As in Adner's blueprint, the levels of risk are represented by red (does not allow for delivery of end value), yellow (requires additional efforts to mitigate risk) or green (does not require additional efforts). The adoption of a meaningful risk analysis method is crucial for the implementation of the cybersecurity blueprint approach. Even though it is out of the scope of the present article, we could mention some points regarding the application of risk analysis methods as part of an ecosystem cybersecurity approach for networked medical devices. First, known risk analysis methods such as Failure Mode and Effect Analysis (FMEA), or Health FMEA (HFMEA) (Shaqdan et al., 2014) do not seem to grasp the full scope of the cybersecurity risks that can be addressed in our ecosystem approach. Approaches based on FMEA-type risk analysis typically address risks due to design failures rather than to malicious attacks. Cybersecurity risk analysis in an ecosystem context needs to address issues associated with intentional malicious agents attacking or interfering with networked medical devices. Secondly, the risk analysis for networked medical devices should focus on the cyber-resilience of the ecosystem, or in other words, the ability to withstand cyber-events or cyber-attacks. Cyber-resilience risks in the context of networked medical devices relate to the control of access, the quality/validity of information, and to the continuity of operation (Boyes, 2015). Risks must also be analyzed within the context of the full lifecycle of networked medical devices and with respect to all relevant stakeholders. In other words, what are the risks related to cases of future, unforeseen cyber-vulnerabilities such as the case of the Heartbleed incident (Krebs, 2014). What is important to point out is the need to move beyond two-dimensional definitions of risk (i.e., probability of harm occurring and severity of the harm once it occurs), which might oversimplify the ability of a medical device company to proactively manage cybersecurity and cyber-resilience risks. Thirdly, the product benefit or utility should be also added to the risk score as a relevant factor. Its addition could provide a higher degree of sophistication of the cybersecurity risk management logic. For example, a risk that remains unacceptable after performing all practicable cybersecurity mitigation measures may actually be tolerable if the device's clinical benefit or medical significance outweighs its residual risks. The next section offers an example case of the application of the value blueprint approach to the analysis of the cybersecurity issues associated with Animas insulin pumps.

Case Study: The Animas Vibe Insulin Pump Cybersecurity Value Blueprint

The described cybersecurity value blueprint was hypothetically applied from the perspective of the manufacturer of the already marketed Animas Vibe Insulin Pump (tinyurl.com/pavb3lp). The Animas insulin pump is used with the G4 PLATINUM Continuous Glucose Monitor made by DEXCOM (tinyurl.com/qda8x5x). The added value of security for the insulin pump has yet to be articulated by manufacturers. In most of the marketing materials, there is little mention of the security of the device, even though the vulnerabilities of insulin pump security have been extensively documented by researchers and presented in the media. The cybersecurity value blueprint would clearly articulate the ecosystem efforts made for improving cybersecurity and provide an additional opportunity for market differentiation.

A Value Blueprint Approach to Cybersecurity in Networked Medical Devices

George Tanev, Peyo Tzolov, and Rollins Apiafi

The Animas insulin pump is an example of the direction towards connected and personal medical devices, which are gaining platform-like properties as they are integrated with other devices and services. The insulin pump is not directly connected to a network, but is connected wirelessly to the glucose monitor, and can transfer data to a healthcare professional via the diasend web service (www.diasend.com/us/) by connecting the pump to a computer via USB or infrared connection. Future networked medical devices will send data to cloud web services wirelessly.

To begin building the cybersecurity blueprint, we first need to establish all of the key elements of the ecosystem. This process is addressed in the first five steps for generating the blueprint. The elements are listed in Table 1.

Following step 2, the cybersecurity blueprint for the Animas insulin pump was generated, as represented in Figure 1.

The security concerns that are highlighted in Figure 1 are graded at the level of "yellow risk" and therefore should be mitigated. The concerns are described below with potential mitigations that could be implemented and their added value reflected in the blueprint:

1. *Cybersecurity management practices of the insulin pump manufacturer:* The manufacturer has to follow a process for assessing and addressing security risks within the device.

   Mitigation: Implementing a cybersecurity management strategy and an open disclosure policy for device security vulnerabilities that have been found by external parties.

2. *Cybersecurity management practices of the continuous glucose monitor manufacturer:* The manufacturer of the Animas pump has limited power over the cybersecurity management practices of their partner device manufacturer. They can assess and address any security issues in the integration process of the two devices.

   Mitigation: None – To be addressed at other locations in the blueprint.

3. *Security implications in the integration of the two devices:* Combining two individual products into a package raises potential security concerns because security for the integrated product was not planned in the initial design process.

Table 1. Key ecosystem elements to be included in cybersecurity value blueprint of Animas insulin pump

Element	Description
End Customer	Patient directly or patient via insurance reimbursement
Your Project	Integrated insulin pump with continuous glucose monitor (from the perspective of insulin pump manufacturers)
Suppliers	Insulin pump mechanical components, hardware, and software
Intermediaries	Regulatory bodies, medical professionals, insurance companies
Complementors	Manufacturer of continuous glucose monitor (DEXCOM) and diasend web service provider

   Mitigation: A third-party firm can be utilized for security tests of the integrated product. This approach can also address vulnerability number 3 from Figure 1.

4. *Regulatory requirements and recommendations of cybersecurity:* The requirements that are set forth by the regulatory body in the region where the product is marketed are relevant for licensing the device. In many regions, there are still no explicit regulatory requirements for cybersecurity.

   M*itigation:* Many of the mitigation steps that are taken for the other vulnerabilities ensure that the manufacturer is not simply fulfilling the bare minimum regulatory requirements, but taking a proactive approach to cybersecurity.

5. *The role and impact of medical professionals on device security:* Medical professionals will most likely play an instructional role with patients and have access to sensitive patient data through web services. It is important that medical professionals are security conscious when dealing with networked devices.

   Mitigation: Training or instructions of good security practices with the device and accessing patient data.

6. *The role and impact of patients/users on device security:* The way that patients operate the device could also risk its security. It is important that patients

A Value Blueprint Approach to Cybersecurity in Networked Medical Devices

George Tanev, Peyo Tzolov, and Rollins Apiafi

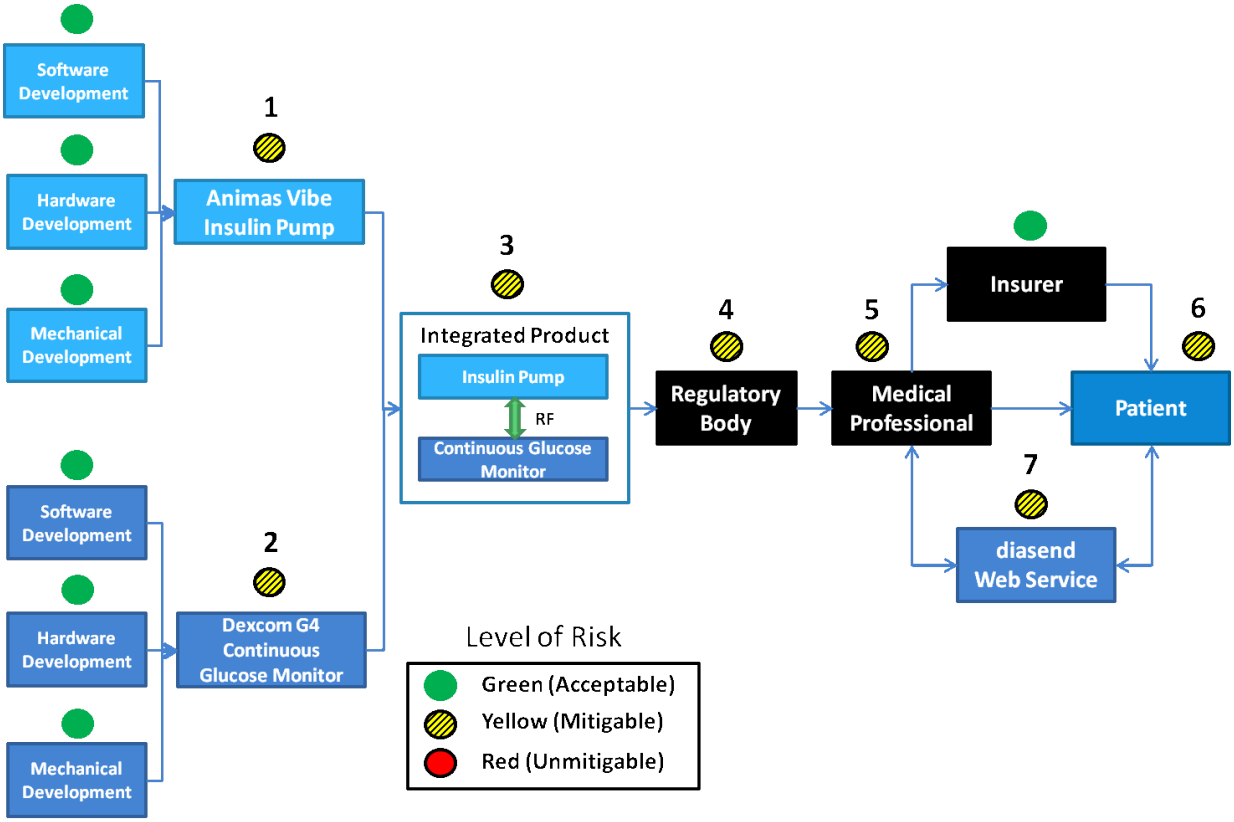

Figure 1. Cybersecurity blueprint for the Animas Vibe insulin pump with numbered locations that have cybersecurity risk levels that need to be mitigated (yellow)

know how to use their device securely and what the risks of compromised security are (e.g., privacy and health risks).

Mitigation: Training or instructions in good cybersecurity practices with the device and clear articulation of the manufacturer's open disclosure policy if they should find any security flaws.

7. *Transferring data between patients and medical professionals over the Internet:* Data that is transmitted from the insulin pump to a computer to upload data to the patient's physician could be susceptible to unauthorized access of the patient's health information. The data can currently be transferred by USB or by infrared data transfer.

   Mitigation: The manufacturer has already made a good choice in using diasend web services that specialize in transferring data between patients and physicians. They also should ensure that any infrared information is encrypted when being transferred.

It is evident that the cybersecurity of networked medical devices is the responsibility of many different stakeholders. When cybersecurity improvement measures are taken in the vulnerable parts of the ecosystem, articulating the value of these efforts is done visually in the blueprint. This type of visual representation of the security value dimension allows stakeholders and end customers to see a manufacturer's comprehensive efforts and highlights the added value and differentiation from competitors. The cybersecurity mitigations have been added to an amended cybersecurity blueprint in Figure 2. The risks that were formerly yellow (mitigable) have been shifted to green (acceptable) following the mitigations that were applied.

Contribution

The key contribution of this article is to extend the value blueprint approach (Adner, 2012) to address the additional value dimension of cybersecurity, in order to articulate cybersecurity value as a way for medical device companies to differentiate in the marketplace.

A Value Blueprint Approach to Cybersecurity in Networked Medical Devices

George Tanev, Peyo Tzolov, and Rollins Apiafi

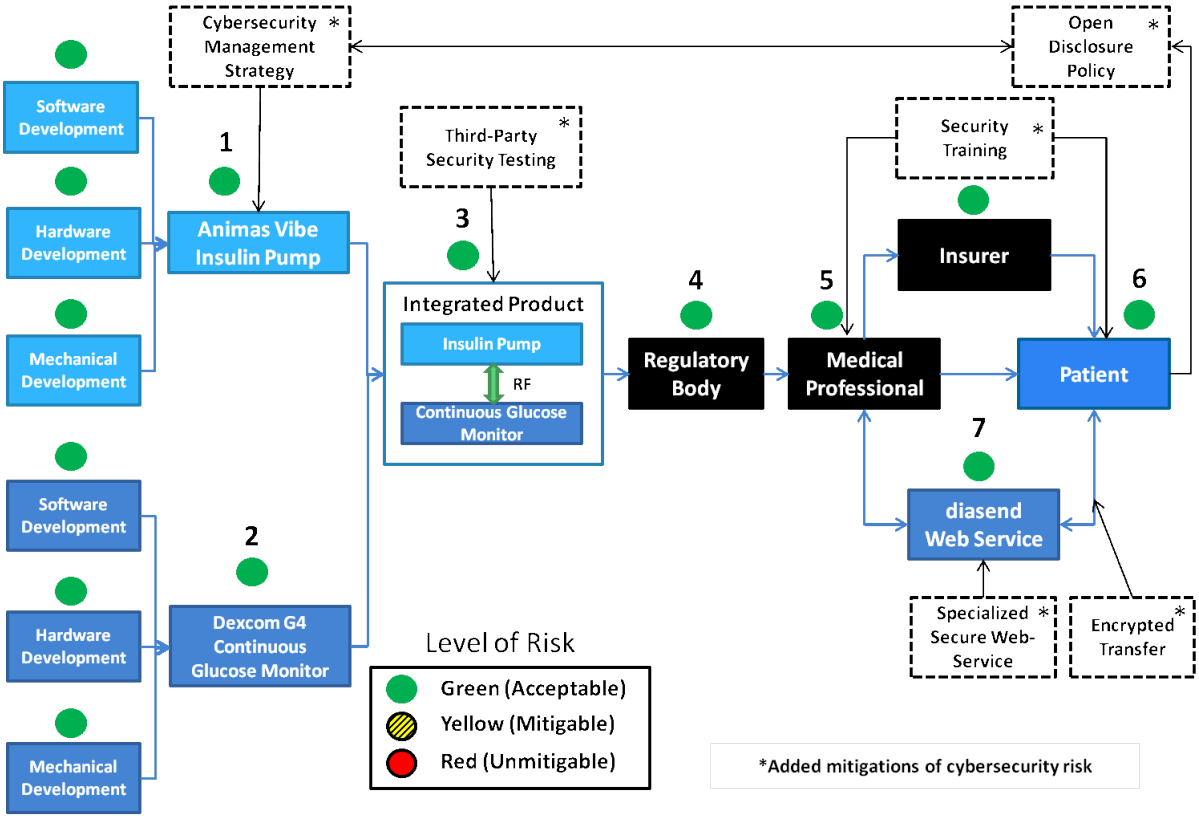

Figure 2. Cybersecurity blueprint for the Animas Vibe insulin pump with added cybersecurity risk mitigations (indicated by a dashed border of the box) and the risk level at the numbered locations reduced to acceptable (green)

The introduction of a cybersecurity value blueprint is important for the following four reasons:

1. It helps in identifying the key stakeholders in the ecosystem together with all associated cybersecurity vulnerabilities.

2. It helps in creating a prioritized plan to address the highest-risk cybersecurity vulnerabilities in collaboration with the rest of the stakeholders.

3. It articulates the value dimensions associated with the security efforts of all relevant stakeholders.

4. It enables innovating the ecosystem through the definition of a clear action plan for improving the security of medical devices over time in a way that could be articulated to business stakeholders and end customers.

This type of approach can change the way security is perceived to become a market differentiator built-in from the onset of design, instead of an add-on at the last stages of the development process.

For future contributions, the method for analyzing the cybersecurity risks within the ecosystem can be explored further. In this work, the emphasis was on establishing the principles for the cybersecurity value blueprint instead of the specific risk analysis, which requires a deeper insight into the various technological platforms enabling the operation of the device. It is clear, however, that the risk analysis within the ecosystem needs to focus on risks associated with the safety, privacy, and security of all stakeholders in the ecosystem. A potential future work could be to adapt a risk analysis method that incorporates cyber-resilience, lifecycle, and utility attributes in the context of networked medical devices and the ecosystem that is identified through the cybersecurity blueprint.

A Value Blueprint Approach to Cybersecurity in Networked Medical Devices

George Tanev, Peyo Tzolov, and Rollins Apiafi

Conclusion

The concern regarding cybersecurity in the increasing number of networked medical devices is growing. Manufacturers have yet to effectively convert their cybersecurity efforts into a market driver and market differentiator. This work argues that not positioning these efforts as a market value and differentiator is a missed opportunity that can be taken advantage of by looking at cybersecurity through an ecosystem perspective rather than a product-centric perspective. The suggested cybersecurity value blueprint approach offers the opportunity to enhance both the "resonating focus" and "points of difference" approach to the articulation of a value proposition by including the cybersecurity value dimension (Anderson et al., 2006). An explicit articulation of cybersecurity provides manufacturers with a tool for localizing and mitigating cybersecurity risks in the ecosystem, and presenting their efforts in a visual blueprint where the value and differentiation can be clearly seen. In an industry where security is beginning to take a central role, and where competition is fierce, the cybersecurity value blueprint could be a tool that would better position manufacturers in the market. Finally, it should be pointed out that, although the suggested tool should be considered as part of a more general risk management approach, it requires deep knowledge of the technological platforms and the specific business process implementation of all involved stakeholders. This is just another illustration of the fact that medical cybersecurity is truly a value co-creation problem that opens new opportunities for technology entrepreneurs and innovation management scholars and practitioners, which should be addressed through the coordinated activities of the entire business ecosystem within a systematic value chain resilience perspective (Boyes, 2015).

About the Authors

George Tanev is a Master of Applied Science candidate in the Technology Innovation Management program at Carleton University in Ottawa, Canada. He holds a Master of Science in Engineering degree in Medicine and Technology from the Technical University of Denmark and a Bachelor's degree in Biomedical and Electrical Engineering from Carleton University. George has industry and research experience in the development of portable medical device products. He also has interests in technology-based entrepreneurship, biomedical signal processing, medical device research and development, medical device regulatory affairs, and medical device cybersecurity.

Peyo Tzolov is a software engineer with a keen interest in entrepreneurship. He holds a Bachelor's degree in Communications Engineering from Carleton University in Ottawa, Canada, and is currently a Master of Applied Science candidate in the Technology Innovation Management program, also at Carleton University. Peyo has several years of experience as a software engineer working on highly scalable and distributed systems. He is very interested in technology, particularly in the security concerns arising from the rapid evolution and adoption of technology.

Tamunoiyowuna Rollins Apiafi is a Master of Applied Science candidate in the Technology Innovation Management program at Carleton University in Ottawa, Canada. He holds a Bachelor's degree in Industrial Chemistry from the University of Port Harcourt, Nigeria. Rollins is one of the co-founders of insight lenz, which specializes in wearable medical technologies that monitors the wearer's eyes to track the state of their health. Rollins is interested in medical device cybersecurity, medical device regulatory bodies, and networked portable medical device research and development.

A Value Blueprint Approach to Cybersecurity in Networked Medical Devices

George Tanev, Peyo Tzolov, and Rollins Apiafi

References

Adner, R. 2012. *The Wide Lens.* London: Penguin Books.

Amin, M., Tariq, Z., & Reed, I. S. 2015. Securing the Car: How Intrusive Manufacturer-Supplier Approaches Can Reduce Cybersecurity Vulnerabilities. *Technology Innovation Management Review,* 5(1): 21–25.
http://timreview.ca/article/863

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

Boyes, H. 2015. Cybersecurity and Cyber-Resilient Supply Chains. *Technology Innovation Management Review,* 5(4): 28–34.
http://timreview.ca/article/888

FDA. 2014. *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff.* Rockville, MD: US Food and Drug Administration.

Fu, K., & Blum, J. 2014. Controlling for Cybersecurity Risks of Medical Device Software. *Biomedical Instrumentation & Technology,* 48(1): 38–41.
http://dx.doi.org/10.2345/0899-8205-48.s1.38

Harries, P. 2014. The Prognosis for Healthcare Payers and Providers: Rising Cybersecurity Risks and Costs. PricewaterhouseCoopers Cybersecurity and Privacy Blog, December 17, 2014. Accessed June 1, 2015:
http://usblogs.pwc.com/cybersecurity/the-prognosis-for-healthcare-payers-and-providers-rising-cybersecurity-risks-and-costs/

Healey, J., Pollard, N., & Woods, B. 2015. The Healthcare Internet of Things: Rewards and Risks. *Atlantic Council,* March 18, 2015. Accessed June 1, 2015:
http://www.atlanticcouncil.org/publications/reports/the-healthcare-internet-of-things-rewards-and-risks

Krebs, B. 2014. 'Heartbleed' Bug Exposes Passwords, Web Site Encryption Keys. *Krebs on Security,* April 8, 2014. Accessed June 1, 2015:
http://krebsonsecurity.com/2014/04/heartbleed-bug-exposes-passwords-web-site-encryption-keys/

Rakitin, S. R. 2009. Networked Medical Devices: Essential Collaboration for Improved Safety. B*iomedical Instrumentation & Technology,* 43(4): 332–338.
http://dx.doi.org/10.2345/0899-8205-43.4.332

Shah, S. 2015. Cybersecurity as a Competitive Differentiator for Medical Devices. M*ed Device Online,* March 24, 2015. Accessed June 1, 2015:
http://www.meddeviceonline.com/doc/cybersecurity-as-a-competitive-differentiator-for-medical-devices-0001

Shaqdan, K., Aran, S., Daftari Besheli, L., & Abujudeh, H. 2014. Root-Cause Analysis and Health Failure Mode and Effect Analysis: Two Leading Techniques in Health Care Quality Assessment. J*ournal of the American College of Radiology,* 11(6): 572–579.
http://dx.doi.org/10.1016/j.jacr.2013.10.024

Wirth, A. 2011. Cybercrimes Pose Growing Threat to Medical Devices. *Biomedical Instrumentation & Technology,* 45(1): 26–34.
http://dx.doi.org/10.2345/0899-8205-45.1.26

Citation: 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

Keywords: cybersecurity, ecosystem, networked medical devices, value proposition, market differentiation

Secure by Design: Cybersecurity Extensions to Project Management Maturity Models for Critical Infrastructure Projects

Jay Payette, Esther Anegbe, Erika Caceres, and Steven Muegge

> *"The challenge in the digital economy is that no chain is stronger than its weakest link."*
>
> Christian Wernberg-Tougaard
> Global Lead for Social Welfare & Human Services
> at Oracle Corporation

Many systems that comprise our critical infrastructures – including electricity, transportation, healthcare, and financial systems – are designed and deployed as information technology (IT) projects using project management practices. IT projects provide a one-time opportunity to securely "design in" cybersecurity to the IT components of critical infrastructures. The project management maturity models used by organizations today to assess the quality and rigour of IT project management practices do not explicitly consider cybersecurity. This article makes three contributions to address this gap. First, it develops the argument that cybersecurity can and should be a concern of IT project managers and assessed in the same way as other project management capabilities. Second, it examines three widely used cybersecurity maturity models – i) the National Institute of Science and Technology (NIST) framework for improving critical infrastructure cybersecurity, ii) the United States Department of Energy's Cybersecurity Capability Maturity Model (C2M2), and iii) the CERT Resilience Management Model (CERT RMM) from the Carnegie Mellon Software Engineering Institute – to identify six cybersecurity themes that are salient to IT project management. Third, it proposes a set of cybersecurity extensions to PjM3, a widely-deployed project management maturity model. The extensions take the form of a five-level cybersecurity capability perspective that augments the seven standard perspectives of the PjM3 by explicitly assessing project management capabilities that impact the six themes where IT project management and cybersecurity intersect. This article will be relevant to IT project managers, the top management teams of organizations that design and deploy IT systems for critical infrastructures, and managers at organizations that provide and maintain critical infrastructures.

Introduction

Cybersecurity attacks on information technology (IT) systems are becoming increasingly frequent and sophisticated (Bailey et al., 2014). *Critical infrastructures* – the assets essential for the functioning of a society and economy (Public Safety Canada, 2009) such as power generation and distribution, transportation systems, healthcare services, and financial systems – are increasingly reliant on networked IT systems (Rahman et al., 2011; Xiao-Juan & Li-Zhen, 2010). Securing these interconnected IT systems from cyber-attack is thus of growing concern to many stakeholders (Merkow & Raghavan, 2012). Security experts argue that security should be "designed in" to critical systems upfront, rather than retrofitted later (Hughes & Cybenko, 2013; McGraw, 2006; Pfleeger et al., 2015).

Cybersecurity capability maturity models (e.g., Caralli et al., 2010; NIST, 2014; U.S. Department of Energy, 2014) are one approach used by organizations to assess capability to defend against cyberattacks, benchmark cybersecurity capability against others, and identify cybersecurity capabilities to improve (Miron & Muita,

Secure by Design: Cybersecurity Extensions to Project Management Maturity Models for Critical Infrastructure Projects *Jay Payette, Esther Anegbe, Erika Caceres, and Steven Muegge*

2014). Like the maturity models in other specialized domains, cybersecurity capability maturity models help organizations to measure their current processes against established industry standards. However, current cybersecurity capability maturity models overwhelmingly focus on evaluating how organizations protect existing systems (i.e., processes to *maintain* cybersecurity) rather than evaluating how organizations securely develop and deploy new secure information systems (i.e., processes to *create* cybersecurity).

New IT systems are typically developed and deployed as *IT projects* (Phillips, 2010), which are managed using project management practices (PMI, 2013a). IT projects provide a one-time opportunity to "design in" cybersecurity to the new IT systems deployed within critical infrastructures. Although the project management domain has its own maturity models (e.g., Sowden et al. 2013; PMI, 2013b), the project management models in use today do not explicitly address cybersecurity. For providers of critical infrastructures and their stakeholders, this is both a gap and an opportunity.

This article makes three contributions to the theory and practice of securing critical infrastructures. First, it develops the argument that cybersecurity can and should be a concern of the IT project managers and project sponsors of critical infrastructure IT projects, and that project management maturity models could be extended to assess cybersecurity capability in the same way that these models assess other capability domains. Second, it identifies six cybersecurity themes that are salient to IT project management. It accomplishes this by selecting three cybersecurity capability maturity models, examining the content and areas of commonality, and identifying those aspects that overlap with the scope of IT project management or are likely to be impacted by project management decisions and activities. The themes therefore reflect both building secure systems and also building systems in secure way. The three models examined are: i) the National Institute of Science and Technology (NIST) framework for improving critical infrastructure cybersecurity, ii) the United States Department of Energy's Cybersecurity Capability Maturity Model (C2M2), and iii) the CERT Resilience Management Model (CERT RMM). Third, it selects a project management maturity model – the PjM3 – and proposes a new five-level cybersecurity capability perspective that augments the seven capability perspectives of the standard model. Bringing together cybersecurity capability maturity models and the PjM3 project management maturity model provides critical infrastructure organizations with the means to evaluate capability in upstream "cybersecurity creation". This approach will be especially useful for organizations that highly value security and concurrently employ cybersecurity capability maturity models to evaluate capability in downstream "cybersecurity maintenance".

The body of this article is structured as four sections. The next three sections each develop one of the article's three contributions and the fourth section concludes.

Securing the IT Project

IT systems within critical infrastructures typically originate as IT projects (Phillips, 2010). Unlike operations, which are continuous and on-going, projects have a specific set of objectives and well-defined and finite time boundaries (Kerzner, 2013). IT development and deployment activities are typically managed using project management tools and techniques, such as those of the Project Management Body of Knowledge (PMBOK; PMI, 2013a), and an IT project management process with well-defined stages and gates between stages (Phillips, 2010).

Decisions and activities within an IT project are likely to have a lasting impact on cybersecurity. Procurement and supply chain management are one example. Outsourced design services, purchase of commercial off-the-shelf (COTS) software, and the adoption of open source software components are all potential sources of vulnerabilities that are difficult to detect and correct later (Ellison et al., 2010). Quality management is a second example. Defects in design, deployment, or provisioning during the IT project could be exploitable until detected and corrected – potentially throughout the active lifecycle of the IT system. The security of the project office and the project infrastructure is also of lasting impact. The tools and processes used for project work, document management, and communication within the project team are all components of information security and integrity. For example, project artifacts thought to be private could be a goldmine to attackers for future social engineering attacks. Thus, IT projects provide a one-time opportunity to securely "design in" cybersecurity to the new IT systems deployed within critical infrastructures.

Capability maturity models approach an activity as a process and formally compare the characteristics of the process in use against the characteristics of an "ideal" process (Humphrey, 1988). This approach originated in

Secure by Design: Cybersecurity Extensions to Project Management Maturity Models for Critical Infrastructure Projects *Jay Payette, Esther Anegbe, Erika Caceres, and Steven Muegge*

software engineering and has been widely applied in many specialized domains, including cybersecurity (Miron & Muita, 2014), capacity to leverage open source software (Carbone, 2007), and enterprise-readiness of open source software projects (Golden, 2008). Project management maturity models are the subset of capability maturity models that focus specifically on project management capabilities. A body of empirical evidence associates the use of project management standards, processes, and maturity models with positive project outcomes (Brookes, 2009; Milosevic & Patanakul, 2005).

The two most developed and widely deployed project management maturity models are:

1. PjM3, the project management component of the Portfolio, Programme, and Project Management Maturity Model (P3M3), maintained by a public–private partnership with the United Kingdom government (Sowden et al., 2013)

2. OPM3, the Organizational Project Management Maturity Model, developed and maintained by the Project Management Institute (PMI, 2013b)

In addition, there are many derivatives of both base models. For example, the PRINCE2 Maturity Model is a specialized derivative of the P3M3 that is specifically aligned with the PRINCE2 (Projects IN Controlled Environments, version 2) project management methodology (Office of Government Commerce, 2009).

Both of these models and their various derivatives address the management of project risks, but none explicitly address cybersecurity. Nonetheless, cybersecurity capability could be assessed at the same time and in the same way as other areas of concern within the scope of project management.

The remainder of this article focuses exclusively on the PjM3 project management capability maturity model. There are three reasons for selecting the PjM3 rather than a different model. First, the PjM3 is the most widely used model internationally (Young et al., 2011). Second, the PjM3 provides a discrete five-level score in seven perspectives (Sowden et al., 2013); discrete and modular models are more easily extensible for our purposes than, for example, the continuous scores of the OPM3. Third, the PjM3 is not explicitly connected with any particular project management framework or process (Sowden et al., 2013); it is thus more widely applicable than specialized models such as PRINCE2. Nonetheless, much of what follows about the PjM3 could be readily adapted to other project management models by repeating the steps described here.

The PjM3 is the project management component of the P3M3 – a broader maturity model that also addresses portfolio management and program management. The P3M3 was developed in 2006 by the Office of Government Commerce in the United Kingdom (OGC, 2006) and was most recently updated in 2013 by Axelos, a private–public partnership with the United Kingdom government (Sowden et al., 2013). It originated as an enhancement to OGC's Project Management Maturity Model, which had been adapted from the original Capability Maturity Model (CMM) developed by the Software Engineering Institute (SEI) in the United States (Humphrey, 1988). P3M3 has been adopted in both government and private organizations. For example, the Australian Department of Finance and Deregulation mandated P3M3 as the common methodology to evaluate Australian government agencies and assess their organizational capability to commission, manage, and realize benefits from ICT-enabled investments (Young et al., 2011).

The PjM3 assesses capability within seven process perspectives (Sowden et al., 2013): i) management control, ii) benefits management, iii) financial management, iv) stakeholder engagement, v) risk management, vi) organizational governance, and vii) resource management. Similar to other process maturity models, each perspective is independently assessed at one of five levels: awareness of process (level 1), repeatable process (level 2), defined process (level 3), managed process (level 4), and optimized process (level 5). Each level and each process perspective has embedded attributes. *Generic attributes* relate to all process perspectives at a maturity level. *Specific attributes* relate only to a particular process perspective. Thus the PjM3 is potentially extensible with new perspectives that employ the same structure and five-level measurement scale, and provide specific attributes for each maturity level.

Cybersecurity Capabilities

There is an extensive body of prior work on cybersecurity and on critical infrastructure that can inform a cybersecurity perspective on IT project management. Miron and Muita (2014) previously identified nine published cybersecurity capability maturity models for critical infrastructures. These nine models were published by five different organizations, with a variety of stated purposes. We employed the following steps to select

Secure by Design: Cybersecurity Extensions to Project Management Maturity Models for Critical Infrastructure Projects *Jay Payette, Esther Anegbe, Erika Caceres, and Steven Muegge*

three models for further examination. First, we scored each of the models identified by Miron and Muita (2014) in five areas: i) maturity and stability of authoring organizations; ii) experience in maturity modelling of authoring organizations; iii) the accessibility of detailed documentation; iv) publishing in the public domain or under open licenses; v) sufficient prescription of framework. Second, we employed three selection criteria: i) high scores in the five areas, ii) no more than one model from any one publisher, and iii) where two models received similar scores, we favoured the more general model or base model over a specialized or derivative model. This selection process was intended to select on both quality and diversity.

The following three cybersecurity capability maturity models were selected for further analysis:

1. The Cybersecurity Capability Maturity Model (C2M2) published by the United States Department of Energy (2014). The first C2M2 model was introduced in 2012, focused specifically on the energy subsector (ES-C2M2). It was updated most recently to version 1.1 in February 2014, and two new variants were launched: a basic sector-neutral version (C2M2; the version used here), and a version tailored to the oil and natural gas subsector (ONG-C2M2). Development was led by the United States Department of Energy (DoE) in partnership with the United States Department of Homeland Security (DHS), and in collaboration with public and private sector experts. C2M2 is structured as ten domains, each comprising a set of cybersecurity practices – the activities that an organization can perform to establish and grow capability in the domain.

2. The NIST Cybersecurity Framework from the National Institute of Science and Technology (NIST, 2014). The NIST Cybersecurity Framework was developed in response to a February 2013 executive order from the United States President to "enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encouraged efficiency, innovation, and economic prosperity" (The President, 2013). It identifies a set of general principles and best practices to guide organizations to develop their own individual readiness profiles.

3. The CERT Resilience Management Model (CERT-RMM) from the Software Engineering Institute (SEI) at Carnegie Mellon University (Caralli et al. 2010). CERT-RMM was the first security model to adopt a capability maturity perspective. Beginning with the first drafts circulated in 2008, and now at version 1.1 (2010), the CERT-RMM was developed as the foundation for a process improvement approach to operational resilience management. It identifies organizational practices necessary to manage operational resilience and to respond to stress with mature and predictable performance.

Table 1 provides a summary of the content and main concerns of each of the three cybersecurity models. There are commonalities among all three models, concerns that are prominent in two of the three models, and unique concerns that are found in one model only.

Next, we systematically identified the cybersecurity concerns from Table 1 that are most salient to IT project management. We eliminated concerns that we deemed as purely operational and retained those concerns that either i) overlap with the scope of IT project management or ii) are likely to be impacted by project management decisions and activities. Finally, we grouped the remaining concerns into broad thematic areas, identifying six project-applicable cybersecurity themes:

1. Project environment security

2. Workforce security knowledge

3. Business continuity planning

4. Secure project supply chain

5. Project deliverable security

6. Project deliverable resiliency

These six themes provide a potential basis for a cybersecurity perspective on project management capability maturity.

Cybersecurity Extensions to the PjM3

To identify the specific attributes of a PjM3 cybersecurity perspective, we re-interpreted the six themes at each of the five levels of generic process-maturity attributes. By employing the same structure and measurement scale, we ensure that the new cybersecurity perspective is fully compatible with the seven standard perspectives of the PjM3, and can be assessed at the same time and in the same way as the standard perspectives.

Secure by Design: Cybersecurity Extensions to Project Management Maturity Models for Critical Infrastructure Projects

Jay Payette, Esther Anegbe, Erika Caceres, and Steven Muegge

Table 1. Content and main concerns of the C2M2, CERT-RMM, and NIST frameworks.

U.S. Department of Energy Cybersecurity Capability Maturity Model (C2M2)	Software Engineering Institute Cyber Risk and Resilience Management (CERT-RMM)	U.S. Department of Commerce NIST Framework for Improving Critical Infrastructure Cybersecurity
• Risk Management	• Resilience Requirements Development	• Asset Management
• Asset, Change, and Configuration Management	• Resilience Requirements Management	• Business Environment
• Identity and Access Management	• Asset Definition and Management	• Governance
• Threat and Vulnerability Management	• Controls Management	• Risk Assessment
• Situational Awareness	• Resilient Technical Solution Engineering	• Risk Management Strategy
• Information Sharing and Communication	• Service Continuity	• Access Control
• Event and Incident Response, Continuity of Operations	• External Dependency Management	• Awareness and Training
• Supply Chain and External Dependencies Management	• Access Management	• Data Security
• Workforce Management	• Identity Management	• Information Protection Processes and Procedures
• Cybersecurity Program Management	• Incident Management and Control	• Maintenance
	• Vulnerability Analysis and Resolution	• Protective Technology
	• Environmental Control	• Anomalies and Events
	• Knowledge and Information Management	• Security Continuous Monitoring
	• People Management	• Detection Processes
	• Technology Management	• Response Planning
	• Monitoring	• Response Communications
	• Organizational Process Definition	• Analysis
	• Organizational Process Focus	• Mitigation
	• Measurement and Analysis	• Response Improvements
		• Recovery Planning
		• Recovery Improvements
		• Recovery Communications

The specific attributes at each of the five maturity levels, are provided in the following five subsections.

Level 1: Awareness

1. There are no cybersecurity training or skills requirements for any project team members.
2. There is no project role responsible for cybersecurity.
3. There is no access or identity control performed on system environments used by the project team.
4. There are no cybersecurity requirements maintained for projects.
5. Project cybersecurity processes such as Statements of Sensitivity (SoS), Threat Risk Assessment (TRA), and Privacy Impact Assessments (PIA) are not performed or are performed in an inconsistent, ad hoc manner.
6. Secure software development practices (e.g., code scans, penetration testing, OWASP) are neither planned nor performed.
7. Projects do not subscribe to organizational procurement standards or processes.

Secure by Design: Cybersecurity Extensions to Project Management Maturity Models for Critical Infrastructure Projects *Jay Payette, Esther Anegbe, Erika Caceres, and Steven Muegge*

Level 2: Repeatable

1. Some team members have cybersecurity skills, but they are applied inconsistently throughout the team.

2. Project documentation is created, but there are no processes to maintain or control project documents or code.

3. Each project is responsible for ensuring appropriate identity and access management of project system environments.

4. Cybersecurity requirements are developed in an inconsistent and ad hoc manner.

5. Project cybersecurity processes (i.e., SoS, PIA, TRA, etc.) are employed in an inconsistent and ad hoc manner.

6. Secure software development practices (e.g., code scans, penetration testing, OWASP) are employed in an inconsistent manner across projects.

7. Business Continuity Plans are inconsistently employed by projects and rarely maintained.

Level 3: Defined

1. Cybersecurity skills are included in the job descriptions of key design, development, and testing roles.

2. Security screening of project resources is performed.

3. Project documentation and code is actively maintained in a secure repository.

4. A project role is identified as responsible for the cybersecurity of project deliverable(s).

5. There are defined processes for access and identity control of all system environments used by the project team.

6. Enterprise cybersecurity requirements are defined at the organizational level and are mandatory for all IT projects.

7. Checklists containing the details of all project cybersecurity processes (i.e., SoS, PIA, TRA, etc.) are available to all project team members.

8. Project standards for secure software development are defined and available to all team members.

9. Project standards for secure management of documentation and code exist and are available to all project team members.

10. Corporate procurement processes are employed by projects and all transactions are auditable.

11. Business Continuity Plan templates are made available to all project team members.

Level 4: Managed

1. Key design, development, and testing resources hold verifiable cybersecurity skills credentials.

2. Access and identity management configurations of project systems environments are consistently audited to ensure environment security and integrity.

3. All requirements documents are reviewed by an enterprise cybersecurity architect.

4. Phase containment exists to ensure that all project cybersecurity processes and standards (i.e., SoS, PIA, TRA, secure software development, Business Continuity Plans, etc.) are appropriately employed by each project and are of appropriate quality.

5. Projects only use qualified vendors who are, among other things, evaluated for security risk.

Level 5: Optimizing

1. Resources for improving cybersecurity skills that pertain to project work are made readily available to the entire project team.

2. A corporate Cybersecurity Centre of Excellence exists to continually improve the cybersecurity capability of project teams.

3. Corporate standards for project cybersecurity processes are continuously improved and actively communicated.

4. Corporate practices for secure software development are continuously improved and actively communicated.

5. Projects actively use their experience to contribute to corporate cybersecurity knowledge.

6. Enterprise cybersecurity requirements are continuously reviewed and improved by a Corporate Cybersecurity Centre of Excellence.

7. An enterprise security architect is required to sign-off on all major project deliverables.

8. Project documentation and code are maintained in a secure repository with strict version control.

9. All project documentation and code artifacts have only one copy, which is maintained in a secure repository.

10. Qualified vendors are continuously evaluated for security risk.

The cybersecurity perspective on project management capability maturity demonstrates the potential relationship between IT project management and cybersecurity of critical infrastructures. Much of the existing work on securing critical infrastructures, including the various cybersecurity maturity models, has emphasized ongoing operations. However, we suggest that an emphasis on operations addresses only half of the cybersecurity challenge, and we argue that the IT projects that design and deploy new IT systems also require attention. Cybersecurity extensions to project management maturity models – such as the PjM3 cybersecurity perspective proposed above – address the introduction of new systems in a way that will be familiar to experienced project managers and project sponsors.

Conclusion

As cybersecurity becomes an increasing area of concern for critical infrastructure providers, governments, and private enterprise, it warrants greater attention from IT project managers, project management offices, and project sponsors. We have argued that IT projects provide an opportunity to securely "design in" cybersecurity to the information systems components of critical infrastructures; thus, cybersecurity can and should be a main concern of IT project managers. A cybersecurity perspective on project management maturity addresses this opportunity in a form that is familiar to project practitioners.

Although this work is presented here at an early stage and has not yet been proven in the field, we sincerely hope that it sparks a dialogue between IT project practitioners, cybersecurity professionals, and providers of critical infrastructures on how to more effectively secure the systems that are essential for the functioning of our society and our economy.

Successful implementation will require action by multiple groups. We call upon IT project managers and project staff to try out these ideas in the field – beginning with informal self-assessments of cybersecurity maturity and followed by action plans to raise scores – and then to report back on their experiences. We call upon critical infrastructure project sponsors to provide IT project managers and project teams with the authority, incentives, training, and resources to "design in" cybersecurity to IT projects and assess the maturity of those efforts. We call upon researchers to empirically test the efficacy of these ideas, particularly the relationships between IT project cybersecurity attributes and high-impact outcomes, including traditional project outcomes, security outcomes, and operational outcomes. If evidence from the field shows this approach to be effective, adoption on a larger scale will require actions from project management organizations to incorporate cybersecurity more formally into the Pj3M and other project management standards. This formalization would open up new revenue opportunities for providers of training services, for providers of certification and assessment services, and for providers of project tools and infrastructure, and it would accelerate the careers of qualified project professions who are capable of operating at a high maturity score on the cybersecurity perspective.

Secure by Design: Cybersecurity Extensions to Project Management Maturity Models for Critical Infrastructure Projects

Jay Payette, Esther Anegbe, Erika Caceres, and Steven Muegge

About the Authors

Jay Payette is a graduate student in the Masters of Design program at Carleton University in Ottawa, Canada, and is the Managing Principal of Payette Consulting. Jay founded Payette Consulting in 2011 to help clients balance the consistent results of repeatable business processes and analytic decision making, with the fuzzy world of creativity. His research has focused on applying design-thinking principles to business model generation, strategy, and project delivery. Prior to founding Payette Consulting, Jay worked for the Canadian consulting practice of Accenture and as an independent IT Project Manager.

Esther Anegbe is a graduate student in the Technology Innovation Management (TIM) program at Carleton University in Ottawa, Canada. She also holds a Bachelor's degree in Computer Engineering from Ladoke Akintola University of Technology in Nigeria. She worked as a Technology Analyst with a leading Investment Management Firm in Lagos, Nigeria (Sankore Global Investments), where she formed part of the technology team that developed, deployed, and provided support for the financial software projects that expanded the market reach of the firm's stock brokerage and wealth management subsidiaries. She is currently working on a startup (Tech Wits) to provide enterprise solutions and services to startups in their accelerators and incubators.

Erika Caceres is a graduate student in the Technology Innovation Management (TIM) program at Carleton University in Ottawa, Canada. She holds a Bachelor's degree in Technology Information Management from The University of Yucatan, Mexico. She previous worked as an innovation consultant at I+D+i Hub, a leading technology transfer office in Merida, Mexico, where she formed part of the management team to produce innovation projects that were submitted for funding to the government to help accelerate the economy in the south of Mexico. She is currently working on Volunteer Safe, an online startup that pre-screens and licenses volunteers and connects them to volunteer opportunities aligned to their profile.

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).

References

Bailey, T., Del Miglio, A., & Richter, W. 2014. The Rising Strategic Risks of Cyberattacks. *McKinsey Quarterly,* May: 17–22. http://www.mckinsey.com/insights/business_technology/the_rising_strategic_risks_of_cyberattacks

Brookes, N., & Clark, R. 2009. Using Maturity Models to Improve Project Management Practice. In *Proceedings from the POMS 20th Annual Conference,* Orlando, FL, May 1–4.

Caralli, R. A., Allen, J. H., & White, D. W. 2010. *CERT Resilience Management Model: A Maturity Model for Managing Operational Resilience* (CERT-RMM Version 1.1). Boston, MA: Addison-Wesley Professional.

Carbone, P. 2007. Competitive Open Source. *Open Source Business Resource,* July: 4–6. http://timreview.ca/article/93

Ellison, R. J., Goodenough, J. B., Weinstock, C. B., & Woody, C. 2010. *Evaluating and Mitigating Software Supply Chain Security Risks.* No. CMU/SEI-2010-TN-016. Software Engineering Institute, Carnegie-Mellon University: Pittsburgh, PA.

Golden, B. 2008. Making Open Source Ready for the Enterprise: The Open Source Maturity Model. *Open Source Business Resource,* May: 4–9. http://timreview.ca/article/145

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

Humphrey, W. S. 1988. Characterizing the Software Process: A Maturity Framework. *IEEE Software,* 5(2): 73–79. http://dx.doi.org/10.1109/52.2014

Kerzner, H. 2013. *Project Management: A Systems Approach to Planning, Scheduling, and Controlling* (11th ed.). Hoboken, NJ: John Wiley & Sons.

Secure by Design: Cybersecurity Extensions to Project Management Maturity Models for Critical Infrastructure Projects

Jay Payette, Esther Anegbe, Erika Caceres, and Steven Muegge

McGraw, G. 2006. *Software Security: Building Security In.* Upper Saddle River, NJ: Addison-Wesley.

Merkow, M. S., & Raghavan, L. 2012. *Secure and Resilient Software: Requirements, Test Cases, and Testing Methods.* Boca Raton, FL: CRC Press.

Milosevic, D., & Patanakul, P. 2005. Standardized Project Management May Increase Development Projects Success. *International Journal of Project Management,* 23(3): 181–192. http://dx.doi.org/10.1016/j.ijproman.2004.11.002

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

NIST. 2014. *Framework for Improving Critical Infrastructure Cybersecurity,* Version 1.0. Gaithersburg, MD: National Institute of Standards and Technology. http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

Office of Government Commerce. 2006. *Portfolio, Programme and Project Management Maturity Model (P3M3).* London: The Stationary Office.

Office of Government Commerce. 2009. *Managing Successful Projects with PRINCE2* (2009 ed.). London: The Stationary Office.

Pfleeger, C. P., Pfleeger, S. L., & Margulies. 2015. *Security in Computing* (5th ed.). Upper Saddle River, NJ: Prentice-Hall.

Phillips, J. 2010. *IT Project Management: On Track From Start to Finish* (3rd ed.). New York: McGraw-Hill.

PMI. 2013a. *A Guide to the Project Management Body of Knowledge* (PMBOK Guide) (5th ed.). Newton Square, PA: The Project Management Institute.

PMI. 2013b. *Organizational Project Management Maturity Model* (OPM3) (3rd ed.). Newton Square, PA: The Project Management Institute.

Public Safety Canada. 2009. *National Strategy for Critical Infrastructure.* Ottawa: Government of Canada. http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-eng.aspx

Rahman, H. A., Martí, J. R., & Srivastava, K. D. 2011. A Hybrid Systems Model to Simulate Cyber Interdependencies between Critical Infrastructures. *International Journal of Critical Infrastructures,* 7(4): 265–288. http://dx.doi.org/10.1504/IJCIS.2011.045056

Sowden, R., Hinley, D., & Clark, S. 2013. *Portfolio, Programme, and Project Management Maturity Model (P3M3): Introduction and Guide to P3M3,* Version 2.1. London: AXELOS Limited. https://www.axelos.com/Corporate/media/Files/P3M3%20Model/P3M3_Introduction_and_Guide.pdf

The President. 2013. *The President of the United States: Executive Order 13636—Improving Critical Infrastructure Cybersecurity.* Federal Register/Presidential Documents, 78(33): February 19, 2013. Washington, DC: U.S. National Archives and Records Administration. http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf

U.S. Department of Energy. 2014. *Cybersecurity Capability Maturity Model* (C2M2 v1.1). Washington, DC: U.S. Department of Energy. http://energy.gov/oe/downloads/cybersecurity-capability-maturity-model-february-2014

Xiao-Juan, L., & Li-Zhen, H. 2010. Vulnerability and Interdependency of Critical Infrastructure: A Review. *Third International Conference on Infrastructure Systems and Services: Next Generation Infrastructure Systems for Eco-Cities (INFRA)*: 1–5. http://dx.doi.org/10.1109/INFRA.2010.5679237

Young, R., Young, M., & Zapata, J.R. 2011. *A Critical Assessment of P3M3 in Australian Federal Government Agencies.* Canberra, Australia: ANZSOG Institute for Governance, University of Canberra. http://www.governanceinstitute.edu.au/magma/media/upload/media/529_P3M3-Anzsig-Insight.pdf

Citation: Payette, J., Anegbe, E., Caceres, 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

Keywords: project management, critical infrastructures, cybersecurity, capability maturity models, CERT RMM, NIST, C2M2, P3M3, PjM3

Representing Botnet-Enabled Cyber-Attacks and Botnet Takedowns Using Club Theory

Olukayode Adegboyega

> *"I don't want to belong to any club that will accept me as a member."*
>
> Groucho Marx (1890–1977)
> Comedian, actor, and host

A model for executing and resisting botnet-enabled cyber-attacks and botnet takedowns does not exist. The lack of this representation results in ineffective and inefficient organizational decision making and learning, hampers theory development, and obfuscates the discourse about the "best-case" scenarios for the future of the online world. In this article, a club theory model for botnet-enabled cyber-attacks and botnet takedowns is developed. Initiatives to execute and resist botnet-enabled cyber-attacks and botnet takedowns are conceptualized as collective actions carried out by individuals and groups organized into four types of Internet-linked clubs: Attacker, Defender, Botbeheader, and Botmaster. Five scenarios of botnet-enabled cyber-attacks and five scenarios of botnet takedowns are examined to identify the specific dimensions of the three constructs and provide examples of the values in each dimension. The developed theory provides insights into the clubs, thereby paving the way for more effective botnet mitigation strategies. This research will be of particular interest to executives and functional personnel of heterogeneous organizations who are interested in improving the quality of their communications and accelerating decision making when solving botnet-related problems. Researchers applying club theory to examine collective actions of organizations linked by the Internet will also be interested in this research. Although club theory has been applied to solve problems in many fields, this is the first effort to apply it to botnet-related problems.

Introduction

A botnet is a network of infected hosts that carry out commands sent by a botmaster. The impacts of botnet-enabled cyber-attacks on individuals and organizations are diverse and have necessitated a collaborative approach that leverages technical and non-technical systems to mitigate botnet-enabled cyber-attacks. However, such collaborative initiatives carried out to solve botnet-related problems are costly, complex, and time consuming due to poor communication among the executives and personnel in technical, legal, security, and research functions of heterogeneous organizations, including law enforcement agencies. Although many collaborative initiatives have been successful, some have not (Lerner, 2014; Schmidt, 2012).

This article provides a representation for executing and resisting botnet-enabled cyber-attacks and botnet takedowns. The intent is to improve communications, learning, and decision making among the various actors that need to come together to effectively and efficiently address botnet-related problems, accelerate theory development, and clarify the discussion about the "best-case" scenarios for the future of the online world.

In this representation, the initiatives to execute and resist botnet-enabled cyber-attacks and botnet takedowns are conceptualized as collective actions carried out by Internet-linked clubs. Collective action refers to actions undertaken for a collective purpose, such as the advancement of a particular ideology or idea, or the polit-

Representing Botnet-Enabled Cyber-Attacks and Botnet Takedowns Using Club Theory

Olukayode Adegboyega

ical struggle with another group (Postmes & Brunsting, 2002). Collective action requires a definition of who "we" are and an understanding of what "we" can do (Drury et al., 2014).

Botnet-enabled cyber-attacks executed by groups such as Wonderland, Anonymous, Drink or Die, The Ukranian ZeuS, Dark Market, Operation Olympic Games, Ghost Net, and PLA Unit 61398 provide examples of collective actions of Internet-linked groups. Membership of such groups is comprised of both willing and unwilling members whose devices were compromised without their consent (Grabosky, 2014).

Other examples of collective action include initiatives to takedown botnets. In 2009, organizations including Defence Intelligence, Panda Security, Neustar, Directi, Georgia Tech Information Security Center, and security researchers came together to form the Mariposa Working Group for the purpose of taking down the Mariposa botnet (Sully & Thompson, 2010). In 2013, Symantec and Microsoft collaborated to obtain a court injunction to dismantle the ZeroAccess botnet (Whitehouse, 2014). In 2014, a group of more than 30 organizations comprised of law enforcement agencies, the security industry, academia, researchers, and service providers cooperated to takedown the GameOver Zeus botnet (Whitehouse, 2014). The group identified the criminal elements and technical infrastructure, developed tools, and crafted messages for users. However, little is known about the inner workings of the collective actions of such groups. By inner working, the author means the arrangement employed by the groups to carry out their activities (e.g., to recruit members or to distribute technical and non-technical infrastructures among members).

Club theory has proven useful in examining the inner workings of collective action in private and public settings (Crosson et al., 2004; Medin et al., 2010). Extant literature on the applications of club theory has focused on non-Internet applications. Club theory has been applied to solve problems related to: highway congestion, highway pricing, provisioning, and financing (Bergias & Pines, 1981; Glazer et al., 1997); grid services (Shi et al., 2006); and the simultaneous deepening and enlargement of the European Union (Ahrens et al., 2005; Thiedig & Sylvander 2000).

A few Internet-related problems such as those related to self-organizing peer-to-peer networks have been solved by the club theory (Asvanund et al., 2004). Raymond (2013) suggested that the Internet can be considered as a set of "nested clubs", and Hofmokl (2010) suggested that Internet goods such as broadband Internet access, proprietary software, and closed databases can be categorized as club goods because they are non-rivalrous in consumption and excludable.

Club theory has been applied to solve problems in many different fields. However, to the author's knowledge, this is the first application of club theory to solve botnet-related problems. In this article, information on five botnet-enabled cyber-attacks and five botnet takedowns are used to conceptualize four types of Internet-linked clubs. The article identifies the dimensions of three constructs and their values observed in ten scenarios.

The remainder of this article is structured as follows. First, the four types of Internet-linked clubs and the three constructs of club theory that anchored the research are described. Then, the method used to carry out the research is explained, and the results are presented. The results include the dimensions of the three constructs for examining the clubs that execute and resist botnet-enabled cyber-attacks and botnet takedowns as well as the characterization of each of the four clubs. The last section provides the conclusions.

Types of Internet-linked Clubs

Definitions of a club has been offered in line with the scope of the authors and the justifications for club formation such as taste for association, and cost reduction derived from team production. A club has been defined as: i) a group of consumers sharing a common facility (Glazer et al., 1997); ii) a group of persons who share in the consumption of a good which is not purely private, nor wholly divisible among persons (Pauly, 1970); iii) a consumption ownership-membership arrangement justified for its members by the economies of sharing production costs of a desirable good (Buchanan, 1965); and iv) a voluntary group of individuals who derive mutual benefit from sharing one or more of the following: production costs, the members' characteristics, or a good characterized by excludable benefits (Cornes & Sandler, 1996). These definitions indicate that a club is a group that shares a good.

A club good has been defined as a good produced and consumed by a group of individuals, whose consumption unit is greater than one but less than infinity (Pauly, 1970); goods that are partially rivalrous and ex-

Representing Botnet-Enabled Cyber-Attacks and Botnet Takedowns Using Club Theory

Olukayode Adegboyega

cludable (Sandler & Tschirhart, 1980); resources from which outsiders can be excluded, for which "the optimal sharing group is more than one person or family but smaller than an infinitely large number" (Strahilevitz, 2006); and goods whose benefits and costs of provision are shared between members of a given sharing arrangement or association (Buchanan, 1965).

A club good has two major characteristics: i) partially rivalrous and ii) excludability. A good is partially rivalrous in consumption when one person's consumption of a unit of the good detracts, to some extent, from the consumption opportunities of another person (Sandler & Tschirhart, 1980). A key feature of the good shared by a club is that it is possible to prevent individuals who have not paid for the good from having access to it. Examples of club goods include hospitals, health clubs, trauma clinics, libraries, universities, movie theatres, telephone systems, and public transport (Sandler & Tschirhart, 1997).

According to club theory, members of a heterogeneous population partition themselves into a set of clubs that best suits their taste for association (Schelling, 1969) and cost reduction derived from team production (McGuire, 1972). Therefore, the individuals and organizations that execute and resist botnet-enabled cyber-attacks and botnet takedowns can be thought of as partitioning themselves into many Internet-linked clubs, each comprised of a group who derive mutual benefits from sharing a good. By "execute" the author means the imposition of rights that were not intended by owners of computer systems, assets, data, and capabilities. By "resist", the author means the enforcement of rights that were intended by owners of computer systems, assets, data, and capabilities. A company such as Microsoft, a law enforcement agency such as the Federal Bureau of Investigations, or a nation state such as China can be members of various clubs, and these clubs can be of different types.

Table 1 shows that the Internet-linked clubs that execute and resist botnet-enabled cyber-attacks and botnet takedowns can be organized into four types based on the nature of the good that members share. Clubs whose members share a botnet belong to Type 1 (Attacker). Clubs whose members share a socio-technical system belong to Type 2 (Defender). Clubs whose members share a botnet termination method to takedown a botnet belong to Type 3 (Botbeheader). Clubs whose members share a command-and-control server network belong to Type 4 (Botmaster).

Type 1: Attacker

Members of an Attacker club share a botnet to compromise or gain unauthorized access to an institution's systems and technology (Gallagher et al., 2014). As introduced earlier, a botnet is a network of bot-infected hosts that carry out commands sent by a botmaster, typically unbeknownst to the owners of the hosts (Yahyazadeh & Abadi, 2015). Botnets are used to carry out cyber-attacks that can cause devastating effects to individuals, organizations, and nation states.

Botnet-enabled cyber-attacks are considered one of the most prevalent and dangerous threats to connected devices on the Internet today. These attacks leverage several thousands of compromised hosts and use complex network structures which are quite difficult to detect, trace and takedown (APEC, 2008; Czosseck et al., 2011; Lerner, 2014). Such malicious activities include distributed denial-of-service attacks (DDoS); Simple Mail Transfer Protocol (SMTP) mail relays for spam; ad-click fraud; and the theft of application serial numbers, login IDs, and financial information such as credit card numbers and bank accounts (Cremonini & Riccardi, 2009; Khattak et al., 2014; Li et al., 2009).

Type 2: Defender

Members of a Defender club share a socio-technical system to detect or counteract the effects of botnet-en-

Table 1. Types of Internet-linked clubs organized by the good members share

Club Type	Shared Good	Main Activity	Activity
1. Attacker	Botnet	Attack using botnet(s)	Execute
2. Defender	Socio-technical system	Defend system(s)	Resist
3. Botbeheader	Termination method	Attack botnet(s)	Execute
4. Botmaster	Command-and-control server network	Control botnet(s)	Resist

Representing Botnet-Enabled Cyber-Attacks and Botnet Takedowns Using Club Theory

Olukayode Adegboyega

abled cyber-attacks. They share the interactions between the social and technical factors that create the conditions that drive organizational performance. Members of this club leverage the socio-technical system to detect deviations from normal activities on systems, identify abuse of systems, mitigate known vulnerabilities, and counteract known threats.

The literature on how to defend against botnet-enabled cyber-attacks highlights the importance of leveraging the diverse skill sets and legal mechanisms available to corporate entities and law enforcement in the form of public–private partnership. For example, the North Atlantic Treaty Organization's (NATO) new cyber-defence policy considers cyber-attacks that threaten any member of the alliance as an attack on all which may provoke collective defense from the alliance's 28 members (Cheng, 2014). In 2000, the defence against cyber-attacks on Estonia was successfully carried out by a working group comprised of the ICT security community, banks, legal authorities, Internet service providers, telcommunication companies, and energy companies (Schmidt, 2012).

Type 3: Botbeheader
Members of a Botbeheader club share a method to terminate a botnet – a particular procedure used to identify and disrupt the botnet's command-and-control infrastructure (Dittrich, 2012; Nadji et al., 2013). Typically, this termination method embodies a legal regime (i.e., a system of principles and rules created by international or domestic law) and is denoted by words such as "behead", "takedown", "takeover", or "eradication" (Dittrich, 2012; Lerner, 2014; Nadji et al., 2013; Sully & Thompson, 2010).

In recent years, governments, not-for-profit organizations, and companies have launched aggressive attacks to disrupt and disable botnets. The techniques used to takedown botnets are as varied as the botnets themselves. Many of the botnet takedown initiatives employ the use of the court system to obtain injunctions to initiate a takedown (Shirazi, 2015).

Type 4: Botmaster
Members of a Botmaster club share one or more command and control servers and a communications network for a particular botnet. These members are called "botmasters".

The botmasters leverage the large network of infected machines, vast underground economy, and forums on the Internet (made possible by the anonymity provided by the Internet) to operate illicit businesses such as false advertising of cheap pharmaceutical drugs, malware distribution, performing a variety of scams, and sending spam emails on behalf of third-party customers (Stone-Gross et al., 2011).

Club Theory Constructs

Club theory is concerned with how groups (clubs) form to provide themselves with goods that are available to their membership, but from which others (non-members) can be excluded. In short, the club theory accommodates the fact that some goods can be simultaneously available to a defined and finite population and subject to explicit exclusion (Crosson et al., 2004).

A construct refers to a single theoretical concept that represents one or several dimensions. Club theory builds on three constructs: i) optimal size of products, ii) optimal membership size, and iii) sharing arrangements. Size is a central characteristic of organizations that is typically measured by the number of employees, members, or total revenues. Sandler and Tschirhart (1980) explain that the optimal size of a product depends positively on its provision level. The greater the value of provision level, the greater the size or number of goods available for consumption. The optimal size of a club is the size at which members derive maximum benefits from the consumption of the shared resource. The sharing arrangements may or may not call for equal consumption on the part of each member, and the peculiar manner of sharing will clearly affect the ways in which the variable enters the utility function. This means that the provisional decisions of the good are based on the contribution of the club members: members who contribute more enjoy a larger share of the club goods (Buchanan, 1965).

Method

The objective of this article is to develop a model for representing botnet-enabled cyber-attacks and botnet takedowns initiatives in terms of the dimensions of the three constructs used in club theory to explain collective action. The model provides insights into the clubs, thereby paving the way for more effective botnet mitigation strategies. To identify the dimensions that can be used to measure the club theory's three constructs and provide examples of the values for each dimension, an interpretative approach to content analysis was used.

Representing Botnet-Enabled Cyber-Attacks and Botnet Takedowns Using Club Theory

Olukayode Adegboyega

The author's interpretation of the results was based on the conceptualization of the four types of Internet-linked club and the three constructs of club theory described above.

A sample comprising 10 scenarios, five for botnet-enabled cyber-attacks and five for botnet takedowns, was selected and the author collected information from the Internet for each of the scenarios in the sample. The information about the scenarios was collected from January 1st, 2009 to December 31, 2014 from sources including: reputable news organizations such as *The New York Times,* CNN, BBC; articles, books, and peer-reviewed research papers; security reports published from well-established security companies such as Kaspersky, Symantec, Defence Intelligence, and Hewlett-Packard; well-established magazine outlets such as T*he Times, Forbes,* and *Foreign Policy.*

Three spreadsheets, one for each construct, were prepared. Each spreadsheet captured the potential dimensions and values collected for the 10 scenarios in the sample. Each scenario had two Internet-linked clubs. Five scenarios focused on botnet-enabled cyber-attacks and included information on two rival Internet-linked clubs, the Attacker and Defender. The five other scenarios focused on botnet takedowns and included information on two rival clubs, the Botbeheader and Botmaster.

The interpretative approach of content analysis was used to identify the sets of dimensions for each construct. A final set of dimensions considered to be essential to a unified representation of botnet-enabled cyber-attacks and botnet takedowns was identified by eliminating ambiguities and inconsistencies. For each dimension, values for each scenario were identified. Finally, these values were used to compare the four types of Internet-linked clubs.

Representation for Executing and Resisting Botnet-Enabled Cyber-Attacks

Figure 1 illustrates a unified representation for executing and resisting botnet-enabled cyber-attacks and botnet takedowns. This representation identifies the eight dimensions that can be used to measure the three constructs from club theory for all four Internet-linked club types.

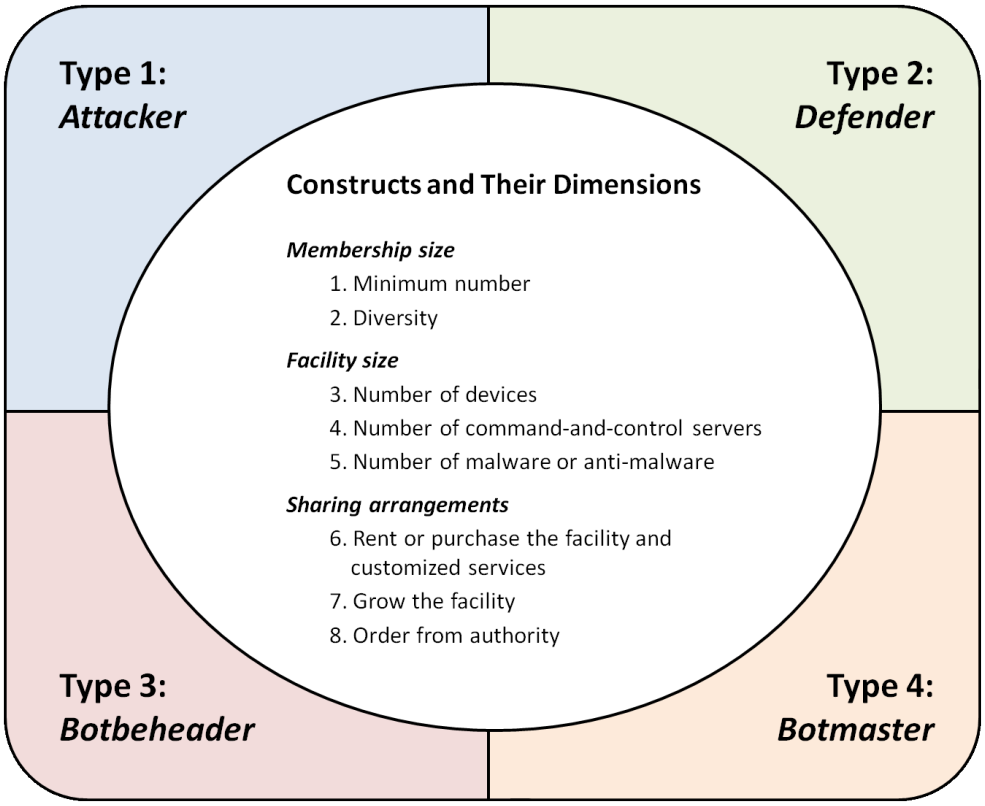

Figure 1. Representation for executing and resisting botnet-enabled cyber-attacks and botnet takedowns

Representing Botnet-Enabled Cyber-Attacks and Botnet Takedowns Using Club Theory

Olukayode Adegboyega

Membership size construct

The construct "Membership size" has two dimensions: minimum number and diversity. "Minimum number" can be measured as: minimum number of individuals and minimum number of organizations. Minimum number of individuals refers to the fewest possible people responsible for executing or resisting cyber-attacks. Minimum number of organizations refers to the fewest possible organization responsible for executing or resisting cyber-attacks. The principle of minimum number was defined by White (1952) and has been used in forensic anthropology and other disciplines. The dimension "Diversity" is a measure of the uniqueness of the entities responsible for executing or resisting cyber-attacks. There exist at least four diversity types: role diversity (e.g., developer, operator, marketer, and accomplices), organization diversity (e.g., private, academic, and government), sector diversity, and country diversity.

Facility size construct

In club theory, facility size is determined by the provision level of the shared resource, which is negatively related to the congestion that characterizes a sharing group (Sandler & Tshirhart, 1997). The results of this research suggest that the construct "Facility size" has three dimensions: number of compromised or end-user devices, number of command-and-control servers, and number of downloadable instances of malware or anti-malware. The dimension "Number of devices" refers to the number of devices leveraged to execute or resist cyber-attacks with or without their owners' consent. The dimension "Number of command and control servers" refers to the number of servers used to issue commands to the computers that are part of the botnet and to accept reports back from compromised computers. The dimension "Number of downloadable instances of malware or anti-malware" refers to the number of software applications and resources used to exploit or defend against vulnerabilities in computer systems.

Sharing arrangements construct

The construct "Sharing arrangements" has three dimensions: arrangements to rent or purchase facility and customized services; arrangements to grow the facility; and arrangements to take order from authority. The dimension "Arrangement to rent or purchase facility and customized services" refers to agreements to derive financial benefits from the use of attack or defence infrastructures. The dimension "Grow the facility" refers to the arrangement to expand infrastructures to execute or resist cyber-attacks. There are at least three means to grow the shared facility: affordable customized products and services, hardware or software capacity upgrade, and network topology that provides control to the owner. The dimensions "Order from authority" refers to the arrangements made with one or more legal authorities to execute or resist botnet-enabled cyber-attacks. Individuals and groups leverage legal frameworks to remain anonymous, takedown botnets, and apprehend and prosecute those who cause botnet-related problems.

Salient Characteristics of Each Club Type

Table 2 provides the results of examining the information collected for the 10 scenarios, five of which focused on botnet-enabled cyber-attacks and five focused on botnet takedowns. For each club type, Table 2 provides the values of the eight dimensions of the three constructs that were extracted from the information collected from the scenarios. For example, for each of the five scenarios in the Type 1 (Attacker) club, the minimum number of individuals who were known to have carried out attacks were 5, 5, 6, 7, and 62. Therefore, the first cell in Table 2 shows the range 5–62. Similarly, the minimum number of organizations collaborating to resist each of these five botnet-enabled cyber-attacks were: 8, 8, 8, 9 and 10. Therefore, the range shown in the second row of Table 2 is 8–10. These results suggest that a Type 2 (Defender) club has at least eight organizations engaged in resisting botnet-enabled cyber-attacks.

The information on the five botnet-enabled cyber-attacks sampled scenarios presented in Table 2 suggests that an Internet-linked Attacker club that fits Club Type 1 (Attacker) is comprised of at least five individuals. Members of this club type assume at least four individual roles to execute cyber-attacks, access millions of compromised devices and downloadable malware programs, use a minimum of one command-and-control server, remain anonymous to evade arrest, use web markets to sell products and services, and grow the facilities members share through access to multiple low-cost customized malware variants.

Also, the five botnet-enabled cyber-attacks scenarios examined suggest that a club that fits Club Type 2 (Defender) club comprises at least eight organizations that act to resist a cyber-attack. These organizations operate in different sectors and countries. These organizations establish contractual agreements for product and service sales, grow their facility using hardware and software upgrades, and actively engage with legal authorities.

Representing Botnet-Enabled Cyber-Attacks and Botnet Takedowns Using Club Theory

Olukayode Adegboyega

The information on the five botnet takedowns sampled scenarios in Table 2 suggests that a Type 3 (Botbeheader) club has at least three organizations engaged in a botnet takedown. These organizations are diverse in terms of operations, sectors, and countries, and they use tens of compromised devices and at least three command-and-control servers. Members of this club type engage in legal and contractual agreements for information sharing and grow the shared facilities via research and development as well as learning from observing information available in web markets.

The results of the five botnet takedown sampled scenarios shown in Table 2 show that the minimum number of members in a club that fits Type 4 (Botmaster) ranges from one to three. These results suggest that this type of club may exists with only one member. Therefore, not all clubs of this type may embody collective action. Members of a club that fits Club Type 4 (Botmaster) have access to at least 500,000 compromised devices, 600,000 downloadable malware programs, and at least one command-and-control server. These members rely on web markets for products and services sales, grow the shared facility using network topologies designed to make botnet takedown difficult, and remain anonymous to evade arrest.

Conclusions

This research applies club theory to examine the collective actions of individuals and groups organized for the purpose of executing or resisting botnet-enabled cyber-attacks and botnet takedowns. The representation developed takes the club theory perspective that collective action can best be understood using three constructs: club membership size; size of the facility that club members share; and arrangements to operate, purchase/rent and grow the shared facility. The representation identifies four Internet-linked club types (i.e., Attacker, Defender, Bottbeheader, and Botmaster) and the eight dimensions of the three constructs of club theory. The representation offered is expected to enhance knowledge on the inner working of the collective actions responsible for executing and resisting botnet-enabled cyber-attacks and botnet takedowns and thereby improves communications among individuals working to solve botnet related problems in heterogeneous organizations and expedite theory development.

Using club theory enhanced our understanding of the various types of Internet-linked clubs that execute and resist botnet-enabled cyber-attacks and botnet takedowns. At least three issues require further research. First, what are the specific learning-related benefits of sharing a botnet, a socio-technical system, a termination method, or a command-and-control server network? The author was not able to extract learning-related benefits from the information collected for the ten scenarios. Thus, answers to the following research questions should be found: How do clubs of the same type learn from one another? How do clubs of different types learn from one another? The author believes that answer to these questions may provide insight to the understanding of inherent motivation for forming and or joining an Internet-linked type of club.

The second area of research entails the study of congestion problems that prevent members of the clubs from deriving maximum benefits from the shared resources. It is surmised that congestion is different across the four club types. For example, congestion in Type 1 (Attacker) clubs may be related more to monetization of products and services in web markets whereas court orders may be causing congestion in Type 3 (Botbeheader) clubs.

The third area of research can focus on the study of the likely rivalry that exists within and among the four types of Internet-linked clubs to offer useful conclusions that can be used to address botnet-related problems.

About the Author

Olukayode Adegboyega holds an MASc degree in Technology Innovation Management (TIM) from Carleton University in Ottawa, Canada and a Bachelor in Electrical and Electronics Engineering from the Federal University of Technology in Akure, Nigeria. He has worked as an IP Network Service Engineer at LM Ericsson Nigeria Limited and as a Data Communication Network Engineer at Globacom Limited of Nigeria.

Representing Botnet-Enabled Cyber-Attacks and Botnet Takedowns Using Club Theory

Olukayode Adegboyega

Table 2. Dimensions of three constructs and examples of their values for each club type

		Botnet-Enabled Cyber-Attacks		Botnet Takedowns	
Dimension		**Club Type 1 Attacker**	**Club Type 2 Defender**	**Club Type 3 Botbeheader**	**Club Type 4 Botmaster**
Minimum number	Individuals	5–62			1–3
	Organizations		8–10	3–8	
Diversity	Role	Developer operator, marketer, and accomplices			Operator
	Organization			Private, academic, and government organizations	
	Sector		Multiple sectors	Multiple sectors	
	Country		Multiple countries	Multiple countries	
Number of devices		50–millions	Tens	Tens	500,000–millions
Number of command-and-control servers		1–2		3–5	1
Number of instances of malware or anti-malware		50–millions	Tens	Tens	600,000–millions
Arrangements to rent or purchase facility and customized services		Web market for selling products and services	Contractual and legal agreements for products and services	Contractual and legal agreements for information sharing and botnet takedown	Web market for selling products and services
Arrangements to grow facility		Affordable and customised malware	Hardware and software capacity upgrade	Web market and R&D for information capturing	Mixture of centralised and de-centralised command-and-control network topologies
Arrangements with legal authorities to execute or resist cyber-attacks		Anonymous to evade arrest	Order to arrest and prosecute culprits	Order to takedown botnet, arrest and prosecute culprits	Anonymous to evade arrest

Representing Botnet-Enabled Cyber-Attacks and Botnet Takedowns Using Club Theory

Olukayode Adegboyega

References

Ahrens J., Hoen, H. W., & Ohr, R. 2005. Deepening Integration in an Enlarged EU: A Club Theoretical Perspective. *Journal of European Integration,* 27(4): 417–439. http://dx.doi.org/10.1080/07036330500367366

APEC. 2008. *Guide on Policy and Technical Approaches against Botnet.* Singapore: Asia-Pacific Economic Cooperation (APEC) Secretariat. http://www.mtc.gob.pe/portal/apectel38/spsg/08_tel38_spsg_012rev1_botnet-guide-version6-4.pdf

Asvanund, A., Krishnan, R., Smith, M. D., & Telang, R. 2004. *Interest-Based Self-Organizing Peer-to-Peer Networks: A Club Economics Approach.* Working Paper: September 2004. Pittsburgh, PA: Carnegie Mellon University. http://dx.doi.org/10.2139/ssrn.585345

Bergias, D., & Pines, D. 1981. Clubs, Local Public Goods and Transportation Models. *Journal of Public Economics,* 15(1): 141–162. http://dx.doi.org/10.1016/0047-2727(81)90030-X

Buchanan, J. M. 1965. An Economic Theory of Clubs. *Economica,* 32(125): 1–14. http://www.jstor.org/stable/2552442

Cheng, J. 2014. Raising the Stakes: NATO Says a Cyber-Attack on One is an Attack on All. *Defense Systems,* September 8, 2014. Accessed June 1, 2015: http://defensesystems.com/Articles/2014/09/08/NATO-cyber-attack-collective-response.aspx

Cremonini, M., & Riccardi, M. 2009. The Dorothy Project: An Open Botnet Analysis Framework for Automatic Tracking and Activity Visualization. *2009 European Conference on Computer Network Defense (EC2ND):* 52–54. http://dx.doi.org/10.1109/EC2ND.2009.15

Crosson, S., Orbell, J., & Arrow, H. 2004. 'Social Poker': A Laboratory Test of Predictions From Club Theory. *Rationality and Society,* 16(2): 225–248. http://dx.doi.org/10.1177/1043463104039878

Czosseck, C., Klein, G., & Leder, F. 2011. On the Arms Race Around Botnets – Setting Up and Taking Down Botnets. *2011 3rd International Conference on Cyber Conflict (ICCC):* 1–14.

Dittrich, D. 2012. So You Want to Take Over a Botnet. In *Proceedings of the 5th USENIX conference on Large-Scale Exploits and Emergent Threats (LEET 2012):* 6. Berkeley, CA: USENIX Association.

Drury, J., Evripidou, A., & Van Zomeren, M. 2014. The Intersection of Identity and Power in Collective Action. In D. Sindic, M. Barreto, & R. Costa Lopes (Eds.), *Power and Identity:* 94–116. Hove, UK: Psychology Press.

Gallagher, H., McMahon, W., & Morrow, R. 2014. Cyber-Security: Protecting the Resilience of Canada's Financial System. *Bank of Canada: Financial System Review,* December 10, 2014. Accessed June 1, 2015: http://www.bankofcanada.ca/2014/12/fsr-december-2014/

Glazer, A., Niskanem, E., & Scotchmer, S. 1997. On the Uses of Club Theory: Preface to the Club Theory Symposium. *Journal of Public Economics,* 65(1): 3–7. http://dx.doi.org/10.1016/S0047-2727(97)00002-9

Grabosky, P. 2014. *Organized Crime and National Security.* RegNet Working Paper, No. 40, Canberra, Australia: Regulatory Institutions Network. http://dx.doi.org/10.2139/ssrn.2464377

Hofmokl, J. 2010. The Internet Commons: Towards an Eclectic Theoretical Framework. I*nternational Journal of the Commons,* 4(1): 226–250.

Khattak, S., Ramay, N. R., Khan, K. R., Syed, A. A., & Khayam, S. A. 2014. A Taxonomy of Botnet Behavior, Detection, and Defense. *Journal of IEEE Communications Surveys & Tutorials,* 16(2): 898–924. http://dx.doi.org/10.1109/SURV.2013.091213.00134

Lerner, Z. 2014. Microsoft the Botnet Hunter: The Role of Public-Private Partnerships in Mitigating Botnets. *Harvard Journal of Law & Technology,* 28(1): 237-261.

Li, Z., Liao, Q., & Striegel, A. 2009. Botnet Economics: Uncertainty Matters. In E. Johnson (Ed.), *Managing Information Risk and the Economics of Security:* 245–267. New York: Springer. http://dx.doi.org/10.1007/978-0-387-09762-6_12

McGuire, M. 1972. Private Good Clubs and Public Good Clubs: Economic Models of Group Formation. *The Swedish Journal of Economics,* 74(1): 84–99. http://www.jstor.org/stable/3439011

Medin, F., Andres, J., Antonio, G. L., & Jesus, L. R. 2010. International Organizations and the Theory of Clubs. *Revista de Metodos Cuantitativos Para La Economia Y La Empresa,* 9(1): 17–27.

Nadji, Y., Antonakakis, M., Perdisci, R., Dagon, D., & Lee, W. 2013. Beheading Hydras: Performing Effective Botnet Takedowns. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security:* 121–132. New York, NY: Association for Computing Machinery. http://dx.doi.org/10.1145/2508859.2516749

Postmes, T., & Brunsting, S. 2002. Collective Action in the Age of the Internet: Mass Communication and Online Mobilization. *Social Science Computer Review,* 20(3): 290–301. http://dx.doi.org/10.1177/089443930202000306

Raymond, M. 2013. Puncturing the Myth of the Internet as a Commons. *Georgetown Journal International Affairs,* Special issue on International Engagement on Cyber III: State Building on a New Frontier, December 23*, 2013:* 53–64.

Sandler, T., & Tschirhart, J. T. 1980. The Economic Theory of Clubs: An Evaluative Survey. *Journal of Economic Literature,* 18(4):1481–1521. http://www.jstor.org/stable/2724059

Sandler, T., & Tschirhart, J. T. 1997. Club Theory: Thirty Years Later. *Public Choice,* 93(1): 335–355. http://dx.doi.org/10.1023/A:1017952723093

Schelling, T. C. 1969. Models of Segregation. *The American Economic Review,* 59(2): 488–493. http://www.jstor.org/stable/1823701

Schmidt, A. 2012. The Estonian Cyberattacks. In J. Healey (Ed.), *The Fierce Domain – Conflicts in Cyberspace 1986-2012.* Washington, DC: Atlantic Council.

Shi, Y., Lau, F. C. M., Tse, S. S. H., Du, Z., Tang, R., & Li, S. 2006. Club Theory of the Grid. *Concurrency Computation,* 18(1):1759–1773. http://dx.doi.org/10.1002/cpe.1027

Representing Botnet-Enabled Cyber-Attacks and Botnet Takedowns Using Club Theory

Olukayode Adegboyega

Shirazi, R. 2015. Botnet Takedown Initiatives: A Taxonomy and Performance Model. *Technology Innovation Management Review,* 5(1): 15–20. http://timreview.ca/article/862

Stone-Gross, B., Holz, T., Stringhini, G., & Vigna, G. 2011. The Underground Economy of Spam: A Botmaster's Perspective of Coordinating Large-scale Spam Campaigns. In *LEET '11 Proceedings of the 4th USENIX Workshop on Large-Scale Exploits and Emergent Threats.*

Sully, M., & Thompson, M. 2010. *The Deconstruction of the Mariposa Botnet.* Ottawa: Defence Intelligence. http://defintel.com/docs/Mariposa_White_Paper.pdf

Thiedig, F., & Sylvander, B. 2000. Welcome to the Club? - An Economical Approach to Geographical Indications in the European Union. *Agrarwirtschaft,* 49(12): 428–437.

White, T. E. 1952. Observations on the Butchering Technique of Some Aboriginal Peoples: I. *American Antiquity,* 337–338.

Whitehouse, S. 2014. Opening Statement. In *Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks.* Washington, DC: U.S. Senate Judiciary Subcommittee on Crime and Terrorism. https://www.hsdl.org/?view&did=756247

Yahyazadeh, M., & Abadi, M. 2015. BotGrab: A Negative Reputation System for Botnet Detection. *Computers & Electrical Engineering,* 41(January): 68–85. http://dx.doi.org/10.1016/j.compeleceng.2014.10.010

Citation: 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

Keywords: botnet, botmaster, botnet takedown, cyber-attack, cybersecurity, collective action

TIM Lecture Series
Three Collaborations Enabling Cybersecurity

Deborah Frincke, Dan Craigen, Ned Nadima,
Arthur Low, and Michael Thomas

> *"Cybersecurity is a huge global issue. And no one organization can solve these problems by itself. We need collaborative approaches. We need to partner. We need ecosystems. We need to bring together our very best. And it's going to take time."*
>
> Dan Craigen
> Science Advisor
> Communications Security Establishment

Overview

The TIM Lecture Series is hosted by the Technology Innovation Management (TIM; timprogram.ca) program at Carleton University in Ottawa, Canada. The lectures provide a forum to promote the transfer of knowledge between university research to technology company executives and entrepreneurs as well as research and development personnel. Readers are encouraged to share related insights or provide feedback on the presentation or the TIM Lecture Series, including recommendations of future speakers.

The third TIM lecture of 2015 was held at Carleton University on May 14th, and was presented by several speakers, each representing different collaborations to enable cybersecurity. In the keynote presentation, Deborah Frincke, Director of Research for the National Security Agency/Central Security Service (www.nsa.gov) in the United States, described the NSA's Research Directorate and its efforts to create breakthroughs in mathematics, science, and engineering that support and enable the wider organization's activities.

Next, Dan Craigen, 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, launched the newest title in the "Best of TIM Review" book series (timbooks.ca), which he co-edited along with Ibrahim Gedeon, Chief Technology Officer at TELUS (telus.com). The book features 15 of the best articles on cybersecurity published in the TIM Review, selected and introduced by the co-editors, and with a foreword from Eros Spadotto, Executive Vice President of Technology Strategy at TELUS. *Cybersecurity: Best of TIM Review* is available for purchase from Amazon (amazon.com/dp/B00XD3O6L0/) in ebook format for Kindle. All proceeds support the ongoing operation of the TIM Review.

Finally, representatives from three companies – Denilson, Crack Semiconductor, and Bedarra Research Labs – described their approaches to collaboration and challenging cybersecurity problems.

Summary

Part I: An introduction to the Research Directorate of the National Security Agency

As Director of Research for the NSA, Frincke leads the only full-spectrum in-house research organization in the United States intelligence community, although its research activities extend beyond the organization through collaborations, linkages, and partnerships with industry, academia, and other government agencies, both within and beyond the United States. The NSA's overall objectives are to:

- defend the vital networks of the United States
- advance the goals of the United States and its alliances
- provide guidance to national decision makers

The Research Directorate engages with leading industries, universities, and national laboratories to both advance core competencies and to leverage work in

TIM Lecture Series – Three Collaborations Enabling Cybersecurity

Deborah Frincke, Dan Craigen, Ned Nadima, Arthur Low, and Michael Thomas

overlapping disciplines. Through the NSA's Technology Transfer Program, the Directorate licenses and shares internally developed technologies with industry, academia, and other government agencies. As examples of such work, Frincke provided an overview of some of the NSA's laboratories and research centres, including:

1. Laboratory for Physical Sciences
   (College Park, Maryland; www.lps.umd.edu)

2. Laboratory for Telecommunication Sciences
   (College Park, Maryland; www.ltsnet.net)

3. Center for Advanced Study of Language
   (College Park, Maryland; www.casl.umd.edu)

4. Research & Engineering
   (Emmerson III, Lavel, Maryland)

5. Laboratory for Analytic Science
   (Raleigh, NC). For details, see the summary of the July 2014 TIM Lecture by David J. Harris (timreview.ca/article/813).

6. The Science of Security online community and network of "lablets" (cps-vo.org/group/SoS)

Finally, Frincke shared some key lessons learned through the activities of the Research Directorate:

1. It is important for a research organization to look ahead, but it must also assess the past and present. A key challenge is to plan for a future where there is an ever-more capable adversary. However, we must also assess technologies that are mature or perhaps past their primes, make decisions about whether or not to continue investing in those technologies, and determine what past activities can be drawn upon for further research.

2. Research must consider the transition paths for new technologies, including research, training, and assistance with culture change. When facing the challenge of managing transitions from the Research Directorate to other directorates, one approach is to embed researchers in missions, which enables learning for new research and transitioning new technology, processes, culture, etc.

3. There is a tendency to always want to "add"; however, doing "new" work means dropping something "old". We try to move on from research that is not coming along fast enough or identify technology that is sufficiently mature that it can be brought out of the NSA for further development.

4. The diversity of classified and unclassified information, research, and devices within the NSA creates a balancing act this is all at once a physical problem (e.g., buildings), a people problem (e.g., access), a technology problem (e.g., security), and a culture problem (e.g., people).

5. We try to invest two-thirds of our efforts into what "the customer" says they want and one-third into what they do not yet know they need or say they do not want, including new, radical innovations.

6. We use strategic forecasting to understand "the outside world", the capacities and capabilities of the adversary, what is happening globally, technology, and investment trends/patterns. We need to make investment decisions along each of these dimensions: how much to invest and when.

Part II: Book launch

Dan Craigen introduced the fourth book in the Best of TIM Review series (timbooks.ca), which was launched at this event. The book stems from five issues on Cybersecurity published in the TIM Review:

1. July 2013 (timreview.ca/issue/2013/july)

2. August 2013 (timreview.ca/issue/2013/august)

3. October 2014 (timreview.ca/issue/2014/october)

4. November 2014 (timreview.ca/issue/2014/november)

5. January 2015 (timreview.ca/issue/2015/january)

These issues represent various research efforts and collaborations led by the Technology Innovation Management (TIM; timprogram.ca) program at Carleton University. In outlining the approach used in the TIM program and illustrated in the articles in the book, Craigen emphasized that technology is only a component of the overall solution to the cybersecurity challenges we are facing today. He stressed that we are as much facing a human behaviour problem as a technology problem. And, he called for multiple disciplines to come together (e.g., sociology, psychology, economics, entrepreneurship) to better understand the developing crim-

TIM Lecture Series – Three Collaborations Enabling Cybersecurity

Deborah Frincke, Dan Craigen, Ned Nadima, Arthur Low, and Michael Thomas

inal markets and related mechanisms. The key messages were that cybersecurity is a global issue and that we need to partner and collaborate, using an ecosystem approach, because no one organization can solve these problems by themselves.

Craigen highlighted that we lack a science of cybersecurity, although this book highlights several steps being taken in that direction. Developing the science will take time, but it will allow us to develop a holistic, proactive approach to replace our current paradigm, which involves simply reacting to new events as though they are independent and do not share any underlying mechanisms or patterns. As evidenced by the articles in this book, efforts are going on to contribute to the science of security, by adding intellectual capacity through courses and research, and through the application of theory to practical problems in the real world.

The book presents different ways of thinking about cybersecurity problems. The hope is that these articles will contribute to theory and provide practical solutions, but also that they will sow the seeds of future research and discussion in different areas. Based on the five special issues published in the TIM Review from 2013 to 2015, the co-editors selected 15 that they feel provide particularly relevant insights into cybersecurity and, in general, contribute to a theory (or science) of cybersecurity. These articles have been divided into three categories:

1. *Understand:* developing and applying models to examine what is happening today to see if it can enhance our understanding

2. *Technical:* trying to advance our approaches on a technical level

3. *Future:* looking out to where we might be in 10 to 20 years and how we might get there

Craigen then illustrated the diversity of thought in the selected articles and put them into context, as he and Ibrahim Gedeon did in the Preface to the book. *Cybersecurity: Best of TIM Review* is available for purchase from Amazon (amazon.com/dp/B00XD3O6L0/) in ebook format for Kindle. All proceeds support the ongoing operation of the TIM Review.

Part III: Company presentations

In the third and final part of the lecture, representatives of three companies shared their current work and collaborations in cybersecurity:

1. Ned Nadina, CEO of Denilson, introduced his company's secure mobile point-of-sale solution for retail enterprises, stressing that a financial technology company needs cybersecurity from day one. Denilson's solution enables credit card payments through the user's mobile hardware, thereby replacing the need for payment terminals.

2. Arthur Low, CEO of Crack Semiconductor, described a lead project through which his company is collaborating. The project, titled Nebular Trusted Provisioning, seeks to develop high-end protection and authentication for intellectual property relating to microchip design software and tools.

3. Michael Thomas, VP of Engineering at Bedarra Research Labs (bedarra.com), described Ivy, which is Bedarra's interactive analytics research environment. It is "an open, interoperable, and extensible platform that combines powerful server-side analytic processing with modern web-based user interfaces for query and visualization". It enables specialists to build customized test suites to allow domain experts to easily and collaboratively explore, analyze, and visualize large datasets using commodity hardware.

TIM Lecture Series – Three Collaborations Enabling Cybersecurity

Deborah Frincke, Dan Craigen, Ned Nadima, Arthur Low, and Michael Thomas

About the Speakers

Deborah Frincke is the Director of Research for the National Security Agency/Central Security Service in the United States. Dr. Frincke's research spans a broad cross section of computer security, both open and classified, with a particular emphasis on infrastructure defense and computer security education. She has been a member of several editorial boards, including: *Journal of Computer Security,* the *Elsevier International Journal of Computer Networks,* and the *International Journal of Information and Computer Security,* and she co-edits a Board column for *IEEE Security and Privacy*. She is a steering committee member for Recent Advances in Intrusion Detection (RAID) and Systematic Advances in Digital Forensic Engineering (SADFE). Dr. Frincke received her PhD from the University of California, Davis in 1992.

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 from Carleton University.

Citation: Frincke, D., Craigen, D., Nadima, N., Low, A., & Thomas, M. 2015. TIM Lecture Series – Three Collaborations Enabling Cybersecurity. *Technology Innovation Management Review*, 5(6): 45–48. http://timreview.ca/article/906

Keywords: cybersecurity, collaboration, NSA, book launch, entrepreneurship, research

Ned Nadima is the Founder and Chief Executive Officer of Denilson, a company that develops mobile payment solutions for retail enterprises. He is currently a graduate student in the Technology Innovation Management (TIM) program at Carleton University in Ottawa, Canada, and he holds a Bachelor's of Science degree in Commerce and Marketing from the University of Ottawa.

Arthur Low is the founder and Chief Executive Officer of Crack Semiconductor, a supplier of high-performance cryptographic silicon IP used in some of the most demanding security applications. Arthur has a number of patents in the field of hardware cryptography. He has worked for a number of IC startups as a Senior IC designer and Architect and gained much of his fundamental IC design experience with Bell-Northern Research in the early 1990s and with IBM Microelectronics in the late 1990s. Arthur has a BSc degree in Electrical Engineering from the University of Alberta in Edmonton, Canada, and is completing his MSc degree in Technology Innovation Management in the Department of Systems and Computer Engineering at Carleton University in Ottawa, Canada.

Michael Thomas is the Vice President of Development at Bedarra Research Labs, a private industrial R&D lab whose mission is to seek out promising next-generation computing and communication technologies and apply them to creative solutions for emerging business problems. Prior to joining Bedarra Research Labs, he worked as a Software Developer and Release Engineer at Object Technology International. Michael holds a Master of Business Administration degree from Athabasca University in Canada, in addition to a Bachelor of Arts degree from Brock University in St. Catharines, Canada.

This report was written by Chris McPhee.

Author Guidelines

These guidelines should assist in the process of translating your expertise into a focused article that adds to the knowledge resources available through the *Technology Innovation Management Review*. Prior to writing an article, we recommend that you contact the Editor to discuss your article topic, the author guidelines, upcoming editorial themes, and the submission process: timreview.ca/contact

Topic

Start by asking yourself:

- Does my research or experience provide any new insights or perspectives?
- Do I often find myself having to explain this topic when I meet people as they are unaware of its relevance?
- Do I believe that I could have saved myself time, money, and frustration if someone had explained to me the issues surrounding this topic?
- Am I constantly correcting misconceptions regarding this topic?
- Am I considered to be an expert in this field? For example, do I present my research or experience at conferences?

If your answer is "yes" to any of these questions, your topic is likely of interest to readers of the TIM Review.

When writing your article, keep the following points in mind:

- Emphasize the practical application of your insights or research.
- Thoroughly examine the topic; don't leave the reader wishing for more.
- Know your central theme and stick to it.
- Demonstrate your depth of understanding for the topic, and that you have considered its benefits, possible outcomes, and applicability.
- Write in a formal, analytical style. Third-person voice is recommended; first-person voice may also be acceptable depending on the perspective of your article.

Format

1. Use an article template: .doc .odt
2. Indicate if your submission has been previously published elsewhere. This is to ensure that we don't infringe upon another publisher's copyright policy.
3. Do not send articles shorter than 1500 words or longer than 3000 words.
4. Begin with a thought-provoking quotation that matches the spirit of the article. Research the source of your quotation in order to provide proper attribution.
5. Include a 2-3 paragraph abstract that provides the key messages you will be presenting in the article.
6. Provide a 2-3 paragraph conclusion that summarizes the article's main points and leaves the reader with the most important messages.
7. Include a 75-150 word biography.
8. List the references at the end of the article.
9. If there are any texts that would be of particular interest to readers, include their full title and URL in a "Recommended Reading" section.
10. Include 5 keywords for the article's metadata to assist search engines in finding your article.
11. Include any figures at the appropriate locations in the article, but also send separate graphic files at maximum resolution available for each figure.

Issue Sponsor