Technology Innovation Management Review

October 2014

Image licensed under CC BY-SA Nick Carter

Cybersecurity

Welcome to the October 2014 issue of the *Technology Innovation Management Review*. This month's editorial theme is 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

Publisher

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

ISSN

1927-0321

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

Editorial: Cybersecurity

Chris McPhee, Editor-in-Chief
Tony Bailetti, Guest Editor

From the Editor-in-Chief

Welcome to the October 2014 issue of the *Technology Innovation Management Review*. This is the first of two issues covering the editorial theme of **Cybersecurity**, and I am pleased to introduce our guest editor, **Tony Bailetti**, Director of Carleton University's Technology Innovation Management program (TIM; timprogram.ca) and Executive Director (Acting) of the VENUS Cybersecurity Corporation (venuscyber.com).

This issue coincides with Cybersecurity Awareness Month in Canada (tinyurl.com/kzb3t27). Previously, we covered the theme of Cybersecurity in July 2013 (timreview.ca/issue/2013/july) and August 2013 (timreview.ca/issue/2013/august). We hope you will read the articles in those issues as well.

In December, we will be publishing an unthemed issue, and I encourage you to get in touch if you would like to submit an article. We hope you enjoy this issue of the TIM Review and will share your comments online. Please contact us (timreview.ca/contact) with article topics and submissions, suggestions for future themes, and any other feedback.

Chris McPhee
Editor-in-Chief

From the Guest Editor

Welcome to the October issue of the TIM Review. The October and November issues examine the theme of Cybersecurity. The contributions published in these two issues are the result of a very intensive industry, university, and government collaboration that started with the launch of the VENUS Cybersecurity Corporation (venuscyber.com) in 2013.

We thank you for reading the journal and urge you to support initiatives to make cyberspace safe, productive, and creative for its users worldwide.

Thirteen authors contributed four articles, a Q&A, and a summary of a TIM Lecture to this issue of the TIM Review. Two of these authors work in industry, five in government, and four in universities. Two of the authors are completing their master program at Carleton University.

Tony Bailetti is at Carleton University; **Renaud Levesque** is Director General and **D'Arcy Walsh** is a Science Advisor at the Communications Security Establishment (CSE). Their article offers a view of a future state of the online world that places safety, productivity and creativity above all else.

Dan Craigen is a Science Advisor, **Nadia Diakun-Thibault** is Senior Science and Analytics Advisor, and **Randy Purse** is the Senior Learning Advisor at the Information Technology Security Learning Centre at the Communications Security Establishment (CSE). These authors propose a definition of cybersecurity that is concise, inclusive, meaningful, and unifying for the purpose of enabling enhanced and enriched interdisciplinary dialectics.

Mika Westerlund, Assistant Professor at Carleton University's School of Business, and **Risto Rajala**, Assistant Professor in the Department of Industrial Engineering and Management at Aalto University in Helsinki, Finland, examine survey data from 109 value-added resellers of a multinational supplier. They show that resellers are more committed to stock and sell cybersecurity products and services if the supplier's digital channel marketing provides tools that help them sell the solutions to end customers.

Editorial: Cybersecurity

Chris McPhee and Tony Bailetti

Walter Miron is a Director of Technology Strategy at TELUS Communications and **Kevin Muita** is a graduate student in the Technology Innovation Management program at Carleton University. Their article examines relevant cybersecurity capability maturity models to identify the standards and controls available to providers of critical infrastructure in an effort to improve their level of security preparedness.

Chen Han is an independent consultant that leads technical teams to develop information system solutions. She and **Rituja Dongre** are both graduate students in the Technology Innovation Management (TIM) program at Carleton University. Their Q&A answers the question: What motivates cyber-attackers?

George Cybenko is the Dorothy and Walter Gramm Professor of Engineering at Darmouth College. He delivered the 6th TIM Lecture of 2014. Cybenko provided an overview of possible security metrics together with their pros and cons in the context of current information technology security practices. He also presented a modelling and simulation approach that produces meaningful quantitative security metrics as the basis for a more rigorous science of cybersecurity.

We encourage the readers of the TIM Review, their colleagues, and their organizations to act decisively to improve the security of cyberspace.

Tony Bailetti
Guest Editor

About the Editors

Chris McPhee is Editor-in-Chief of the *Technology Innovation Management Review*. Chris holds an MASc degree in Technology Innovation Management from Carleton University in Ottawa and BScH and MSc degrees in Biology from Queen's University in Kingston. He 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.

Tony Bailetti is an Associate Professor in the Sprott School of Business and the Department of Systems and Computer Engineering at Carleton University, Ottawa, Canada. Professor Bailetti is the Director of Carleton University's Technology Innovation Management (TIM) program. His research, teaching, and community contributions support technology entrepreneurship, regional economic development, and international co-innovation.

Citation: McPhee, C., & Bailetti, T. 2014. Editorial: Cybersecurity. *Technology Innovation Management Review*, 4(10): 3–4. http://timreview.ca/article/833

Keywords: future vision, online, Internet, Internet of Things, Industrial Internet, Internet of Everything, safety, security, cybersecurity, productivity, excludability, rivalry, bisociation

The Online World of the Future: Safe, Productive, and Creative

Tony Bailetti, Renaud Levesque, and D'Arcy Walsh

> *"A mind is like a parachute. It doesn't work if it is not open."*
>
> Attributed to Frank Zappa (1940–1993)
> Musician, composer, producer, and director

A safer online world is required to attain higher levels of productivity and creativity. We offer a view of a future state of the online world that places safety, productivity, and creativity above all else. The online world envisaged for 2030 is safe (i.e., users communicate with accuracy and enduring confidence), productive (i.e., users make timely decisions that have an ongoing global effect), and creative (i.e., users can connect seemingly unrelated information online). The proposed view differs from other views of the future online world that are anchored around technology solutions, confrontation, deception, and personal or commercial gain. The following seven conditions characterize the proposed view of the online world: i) global-scale autonomous learning systems; ii) humans co-working with machines; iii) human factors that are authentic and transferrable; iv) global scale whole-brain communities; v) foundational knowledge that is authentic and transferrable; vi) timely productive communication; and vii) continuous technological adaptation. These conditions are expected to enable new social-behavioural, socio-technical, and organizational interaction models.

Introduction

The nature of the online world of the future is best understood by explaining the properties of safety, productivity, and creativity. Understanding these properties requires more than technology debates. Although technology is indeed important, today we have a unique opportunity to shape the future of the online world for the greater good. However, we must understand the underlying causes of the complexity that is emerging as layers of cognition, computation, and connection evolve.

We illustrate our vision as a shift over time towards increased safety and situational understanding. As Figure 1 shows, we are now living in an unsafe world with limited situational understanding. The shift over time shows us reaching the future state by first moving to a safer world with increasing situational understanding (i.e., machines are connected but humans and machines are only loosely connected) and then moving to a safe world that provides more situational understanding (i.e., human-machine convergence, awareness, and autonomy). As a result of this shift, we envision a future

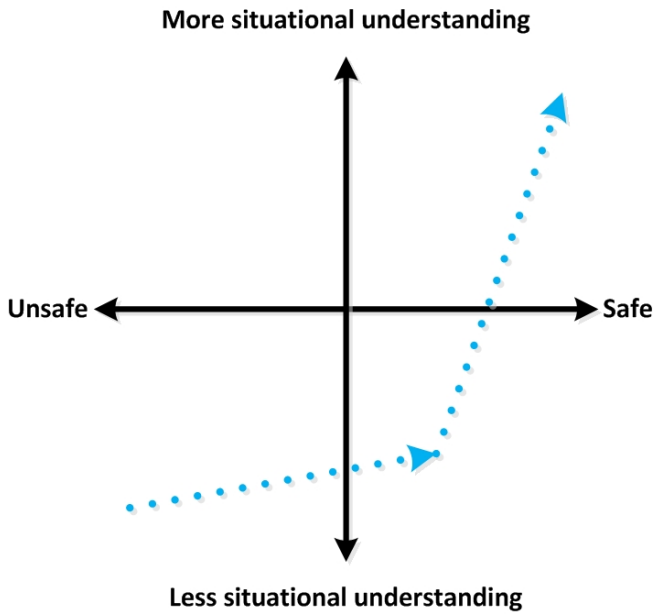

Figure 1. Progression from today's environment to our vision of the future online world in 2030

The Online World of the Future: Safe, Productive, and Creative

Tony Bailetti, Renaud Levesque, and D'Arcy Walsh

environment in which: i) productivity is uniquely enabled through instantaneously and safely connecting information elements and ii) transformational creativity is uniquely enabled through instantaneously and safely connecting together seemingly unrelated information.

In this article, we share our vision of the online world of the future by first describing safety, productivity, and creativity and then identifying the set of key conditions of a safer environment expected to enable unprecedented levels of productivity and creativity in the future. Further, we explore how the key conditions depend on one another and provide an example scenario to illustrate a domain-specific application that satisfies these conditions. Finally, we present the progression from today's environment to our vision of the future online world and position competing views of the future online world in terms of excludability and consumption rivalry using quadrant-style representations.

This article makes three contributions. First, it explicitly links safety properties to significant increases in productivity and creativity. Second, it postulates a set of research questions that should be answerable if the underlying properties of safety, productivity, and creativity are adequately understood. Third, the article identifies a set of key conditions of the online world of the future.

Online World of the Future

This section describes safety, productivity, and creativity in the context of the online world of the future.

Safety

To unleash unprecedented levels of productivity and creativity, the online world of the future must be safe (i.e., enable communication with accuracy and with enduring confidence). To be safe, the online world must be protected from: i) pernicious actors (e.g., individuals, groups, organizations, or nation-states) that strive to undermine and to unjustly benefit from the work of others, and ii) unintended disruption (e.g., user errors that have negative side effects) (Leveson, 2013). If Maslow's hierarchy of needs can be addressed with technology (Gerstein, 2014), information may be utilized as a foundational element that is authentic and is transferrable to others – in a manner that is beneficial to the world at large.

The online world of today is not engineered for safety (Leveson, 2013). We benefit from state-of-the-art knowledge of the theory and practice of safety properties in the context of cybersecurity, especially from a technical perspective. However, it is clear to us that there is no underlying theory that explains cybersecurity-related phenomena within the technical domain let alone associated safety properties that include dynamic and social characteristics, which are widely viewed to be more important than technical ones. Existing theories apply to restricted sub-domains of the overall problem space, such as cryptography, and therefore only explain phenomena within highly restricted contexts that do not have the semantic power or scope to explain other safety-related properties that concern the behaviour of the adversary and the behaviour of those who are under attack (Craigen et al., 2013).

If an underlying theory of safety existed, the following example research questions, amongst many others, would be answerable:

- Under what conditions does an attacker have an advantage over an infrastructure protector?
- Why do many infrastructure protectors and users not adopt effective mechanisms to provide safety and privacy?
- What are the resources, processes, and values to concurrently provide online safety and privacy to users?
- What are the characteristics of the individuals and organizations that are most likely to attack?
- What are the enhanced characteristics of safety through disclosure (i.e., by being open and not by being proprietary)?

Productivity

Productivity is inherently based on association or association by similarity or co-occurrence (Dubitzsky et al., 2012). We adopt the perspective that productivity is related to the efficiency and effectiveness of understanding and utilizing existing connections amongst known information elements. This view implies that information has been pre-selected to serve a purpose that is already defined and whose utility is already appreciated. Supporting technologies focus and simplify information relevant to a user's task that can accommodate discovery but within a relatively closed context. Compared to creativity gains, which are new, surprising, and of value, productivity gains, which are more conventional in nature, happen under routine conditions that are already known (Dubitzsky et al., 2012).

The Online World of the Future: Safe, Productive, and Creative

Tony Bailetti, Renaud Levesque, and D'Arcy Walsh

We foresee a future environment in which productivity is fundamentally enabled through instantaneous and safe connections among information elements. Productivity gains will remain conventional in nature but will happen in a profoundly different way. Users will be able to make timely decisions that have an ongoing global effect when information is available instantaneously, with accuracy and with enduring confidence, and senders and receivers of information are available instantaneously on a global scale. Achieving this level of productivity will require global-scale systems that interact to learn and converge on solutions autonomously when constantly assessing the meaning of connections that are known to exist amongst known information elements.

If an underlying theory of productivity existed, the following example research questions would be answerable:

- How do individuals in groups create reference frames that anchor their actions?
- How can we improve organizational performance through collective knowledge?
- How does communicating with fidelity and with enduring confidence specifically relate to productivity?
- Which communications are urgent or important?
- How are instantaneous communications and timely decisions, which can have a global effect, synchronized?

Creativity

Psychologists and neuroscientists are actively investigating the process of creativity. The work of Andreasen (2005); Csikszentmihalyi (1996); Gilovich, Griffin, and Kahneman (2002); and Kahneman (2011) are examples of well-known research within these two areas. Duxbury (2012) assesses the process of creativity and its relationship to innovation. Cognitive and computer scientists are investigating how computers can be designed to autonomously manipulate abstract concepts while Boden (1999) is concerned with computer models of creativity.

Transformational creativity constitutes the deepest form of creative processes in Boden's (1994) model of creativity. Transformational creativity leads to breakthroughs because established conceptual spaces or thinking styles, which limit types of thought, are transformed so that thoughts that were inconceivable within existing conceptual spaces are now possible (Dubitzsky et al., 2012). This level of creativity requires connecting seemingly unrelated information through computational creativity (Boden, 1999), bisociation (Koestler, 1964), and other approaches. These approaches lead to new, surprising, and valuable breakthroughs when normally distinct and unrelated contexts or categories of objects are mixed in one human or machine mind. Bisociation goes beyond associative styles of thinking that are based on established routines (Dubitzsky et al., 2012).

In the online world of the future, instantaneous and safe connections among seemingly unrelated information will enable transformational creativity. Humans and machines will be able to: i) communicate with accuracy and with enduring confidence and ii) make timely decisions that have an ongoing global effect. Through computational creativity and human-machine convergence, humans and machines will learn together to discover new knowledge and to assess (un)certainty.

If an underlying theory of creativity existed, the following example research questions, amongst many others, would be answerable:

- How do people working in creative domains employ creative thinking to connect seemingly unrelated information?
- What does it mean to combine elements from incompatible domains to generate creative solutions and insight?
- How do you teach humans or machines to be creative?
- How do you develop machine-based solutions that support creative thinking?
- How can machines be used to define and construct artificial conceptual spaces that generate creative insight and solutions?

Seven Conditions and Their Interdependencies

The conditions listed below characterize our view of the online world of the future. Together, they are intended to comprise the circumstances of a safer environment that will foster unprecedented levels of human-machine creativity and productivity. Within this online environment, the intellectual capacities of humans and machines converge for the betterment of humankind through unified knowledge, instantaneous communica-

The Online World of the Future: Safe, Productive, and Creative

Tony Bailetti, Renaud Levesque, and D'Arcy Walsh

tions, and continuous change, which together lead to transformational creativity. This list has been formulated based on our collective knowledge and experience.

The key conditions of the online world of the future that enables a new level of creativity, productivity, and safety for humans worldwide are:

1. *Global-scale autonomous learning systems:* Systems and networks will continuously learn at a global scale and therefore will adapt their interactions to autonomously interpret new information and to discover new knowledge, including automatically assessing the uncertainty of this new information or knowledge.

2. *Humans co-working with machines:* Humans (providing insight and understanding) and systems/networks (interpreting information at scale) will interwork to assess and to achieve joint goals to predict continuously emerging complex phenomena.

3. *Human factors are authentic and transferrable:* Cognitive characteristics, which indicate how people think, how people interact, and how societies and groups behave, will be inherent within interactions, allowing communication with fidelity and therefore with confidence.

4. *Global-scale whole-brain communities:* Societal formations, which provide human-driven informed insights, will emerge, interact, and disband in a manner that is open and appropriately beneficial to community participants so that the right minds can work on the right problems at the right time.

5. *Foundational knowledge is authentic and transferrable:* Creative and productive outcomes are propagated independently of the lifetime of particular individuals or organizations; the future interpretation of these productive outcomes may happen safely.

6. *Timely productive communication:* Every contemplated interaction can happen appropriately and instantaneously with knowledge of other interactions or previous creative and productive outcomes.

7. *Continuous technological adaptation:* The online world of the future, as a safe system of systems, dynamically evolves to enable creative and productive outcomes, including the incremental transformation of the world of today to a fully digitally enabled society of the future.

We consider these conditions as a starting position. They should be continuously validated, refined, and adjusted as progress is made evolving underlying theories, as technological solutions are researched and developed, and as detailed field trials are conducted over time.

Interdependencies

Figure 2 illustrates how the seven conditions identified in the previous section relate to one another.

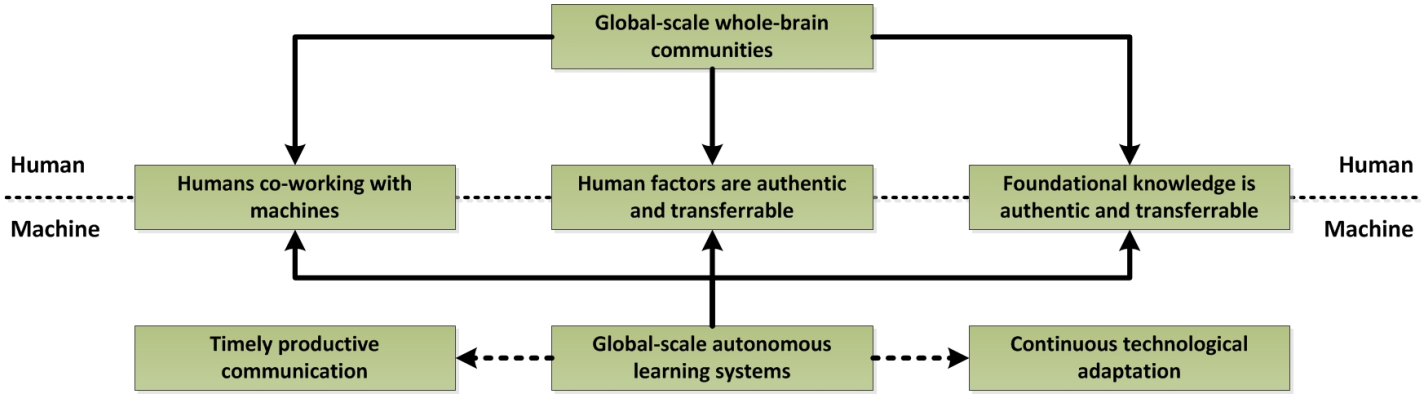

Figure 2. Dependencies among the seven conditions of the online world of the future

The Online World of the Future: Safe, Productive, and Creative

Tony Bailetti, Renaud Levesque, and D'Arcy Walsh

In our view of the online world of the future, Condition 1 (*Global-scale whole-brain communities*) is purely a human-oriented condition. Three conditions are part of the human-machine divide: Condition 2 (*Humans co-working with machines*), Condition 3 (*Human factors are authentic and transferrable*), and Condition 5 (*Foundational knowledge is authentic and transferrable*). Finally, three conditions are purely systems/network conditions: Condition 4 (*Global-scale autonomous learning systems*), Condition 6 (*Timely productive communication*), and Condition 7 (*Continuous technological adaptation*).

Figure 2 indicates that *Global-scale whole-brain communities* and *Global-scale autonomous learning systems* are two control points; the former is driven by humans and the latter is driven by systems/networks. These two conditions depend on each other through their direct dependence with *Humans co-working with machines*, *Human factors are authentic and transferrable*, and *Foundational knowledge is authentic and transferrable*. Within the scope of systems/networks, *Global-scale autonomous learning systems* directly depends on *Timely productive communication* and *Continuous technological adaptation*.

An Example

Here, we offer an example scenario of the online world of the future. The scenario describes the dynamic interoperation of two initially decoupled financial systems that specialize in maintaining knowledge and providing predictions about the energy sector of the economy. Consider two global-scale financial analysis systems – System A and System B – in which value is being created based on the present-value analysis of future cash flows. Each system is, in essence, implementing a future-oriented process that projects current economic performance over a time span applicable to the nature of a given business activity and its market segment. In such projections, there is often a distinction made between shorter-term and longer-term predictions and any analytic outputs may be indicator- or magnitude-based information. In this context, data-driven change that minimizes human intervention and bias must be systematically integrated with human-driven information that is the result of naturally adaptive and perceptive processes.

The clients who use System A are concerned with shorter-term predictions. The clients who use System B are concerned with longer-term predictions. Each system provides results of scenario analyses, knowledge about the energy sector and its conditions, cash flow projections, and valuation assessment for the shorter- or longer-term timeframes. For timeliness, System A projects cash flow and assesses valuations online and in real time. For greater accuracy, System B projects cash flow and assesses valuations offline and on demand.

These two systems are *global-scale autonomous learning systems* that can safely communicate with accuracy and with enduring confidence. Through known connections with known information elements in the financial domain, these two systems discover each other and establish a dynamic connection to interoperate in order to leverage each other's preferred stock predictions. System A is now able to use System B's longer-term predictions to validate its shorter-term predictions. System B is now able to use System A's shorter-term predictions to validate its longer-term predictions. This scenario provides an example of productivity gains through timely decisions that have an ongoing global effect. The predictions made by both systems have now been markedly improved. This interaction has happened autonomously because of *timely productive communication* and the dynamic reconfiguration of each system is an example of *continuous technological adaptation*.

Now consider human-driven information that is the result of naturally adaptive and perceptive processes. Because *human factors are authentic and transferrable* and *foundational knowledge is authentic and transferrable*, the human specialists of System A and System B have not only been alerted to the improved accuracy of their system's predictions but also to the human factors, the cognitive conditions, which led to how and why these new predictions were made. Because the human specialists of System A and System B are *humans co-working with machines*, they may interact with their respective systems to clarify any ambiguities or apparent contradictions and to more deeply understand the implications with respect to how they must adjust, from a human-driven information perspective, their shorter- or longer-term predictions. The new information may be utilized as *foundational elements that are authentic and are transferrable* because the two systems safely communicated with accuracy and with enduring confidence.

Finally, because they now know about each other and understand how and why each other came to the conclusions they came to, a specialist of System A and a specialist of System B, who live in very different parts of

The Online World of the Future: Safe, Productive, and Creative

Tony Bailetti, Renaud Levesque, and D'Arcy Walsh

the world, start working together as a *global-scale whole-brain community* to assess any remaining ambiguities or contradictions. To resolve one contradiction, for example, one of the specialists has the sudden insight to analyze the situation from a completely different perspective by working with another specialist who is an expert in smart grids and distributed control systems for the energy sector. Acting as a *global-scale whole-brain community*, the three analysts are able to formulate a set of unique hypotheses, which they plan to test at scale through having the financial analysis systems interact in a restricted manner with the energy control systems of the companies that were associated with their financial predictions. This is an example of breakthrough thinking by connecting seemingly unrelated information.

As *humans co-working with machines*, they ensure, through *human factors are authentic and transferrable* and *foundational knowledge is authentic and transferrable* that the shorter- and longer-term predictions of their respective systems reflect this new knowledge and the thinking that was required to understand how and why this was the case.

Differentiation

In this section, we compare our view of the future of the online world and three competing visions: the Industrial Internet (Annunziata, 2013), the Internet of Things (Wikipedia, 2014), and the Internet of Everything (Cisco Systems, 2014). Figure 3 positions the four views of the future of the online world in terms of their excludability and consumption rivalry. These distinctions are important because they guide human action, and humankind can choose what to do with the Internet. For example, humankind can make Internet access similar to:

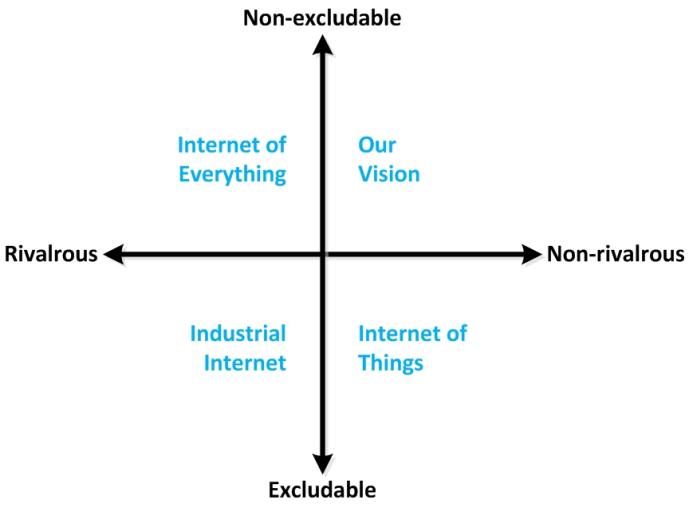

Figure 3. Positioning competing views of the future online world

1. *air:* difficult to exclude, low rivalry

2. *public parks:* easy to exclude, low rivalry

3. *food:* easy to exclude, high rivalry

4. *fish stocks:* difficult to exclude, high rivalry

Today, depending on location, access to the Internet may follow any one of these four analogies.

Figure 3 indicates that the Industrial Internet will exclude many from benefiting from what it has to offer and will increase rivalry among the few. Our vision is represented as air; you cannot exclude people from breathing air and breathing as much air as you want does not take away the air that others breathe. There is the same technological underpinning for both cases, but very different economic models apply.

Consider further that the Internet goes beyond just access. Humankind has more choices to make, because the Internet also encompasses social and cultural issues, including intellectual property rights and ethical concerns. In general, we can think of the Internet, like other systems, as having three layers composed of the cognition, computation, and connection layers (Tibbs, 2013). Today, for Western society, most elements of the connection layer are like food (easy to exclude, high rivalry), most of the elements of the cognition layer are like parks (easy to exclude, low rivalry), and most elements of the computation layer are like fish stocks (difficult to exclude, high rivalry).

Conclusion

The safety of the online world of the future is an important precondition for a profound enhancement of human productivity and creativity by 2030. Safety properties of the online world of the future must ensure information elements are authentic and transferable to others at a global scale of interaction. We believe that, through association, enhanced productivity will be achieved by safely and instantaneously connecting known information elements, including by autonomous learning systems that operate at a global scale. We believe that, through bisociation, enhanced creativity will be achieved by safely and instantaneously connecting information elements that were previously viewed

The Online World of the Future: Safe, Productive, and Creative

Tony Bailetti, Renaud Levesque, and D'Arcy Walsh

to be disparate in nature, including through computational creativity and human-machine convergence.

When making progress towards understanding the scientific underpinnings of the online world of the future, we have presented a set of example research questions that we believe should be addressed or further refined. We have also presented the progression from today's environment to our vision of the future online world and positioned competing views of the future online world in terms of excludability and consumption rivalry using a quadrant-style representation.

Finally, if machines and humans are to interact and collaborate more systematically, we need to start thinking about the ethical values – and not only the creative and productive skills – that will be assigned to these machines when the outcomes of their decisions will apply to human populations, in the sense that solutions that are productive from a collective perspective can erode individual freedoms.

About the Authors

Tony Bailetti is an Associate Professor in the Sprott School of Business and the Department of Systems and Computer Engineering at Carleton University, Ottawa, Canada. Professor Bailetti is the Director of Carleton University's Technology Innovation Management (TIM) program. His research, teaching, and community contributions support technology entrepreneurship, regional economic development, and international co-innovation.

Renaud Levesque is the Director General of Core Systems at the Communications Security Establishment (CSE) in Ottawa, Canada, where he is responsible for R&D and systems development. He has significant experience in the delivery of capability and organizational change in highly technical environments. His career began at CSE in 1986 as a Systems Engineer, responsible for the development and deployment of numerous systems, including the CSE IP corporate network in 1991. In 2000 Renaud went to work in the private sector as Head of Speech Technologies at Locus Dialogue, and later at Infospace Inc., where he became Director of Speech Solutions Engineering. He rejoined CSE in 2003, where he assumed the lead role in the IT R&D section. Subsequently, as a Director General, he focused efforts towards the emergence of CSE's Joint Research Office and The Tutte Institute for Mathematics and Computing. Renaud holds a Bachelor of Engineering from l'École Polytechnique, Université de Montréal, Canada.

D'Arcy Walsh is a Science Advisor at the Communications Security Establishment (CSE) in Ottawa, Canada. His research interests include software-engineering methods and techniques that support the development and deployment of dynamic systems, including dynamic languages, dynamic configuration, context-aware systems, and autonomic and autonomous systems. He received his BAH from Queen's University in Kingston, Canada, and he received his BCS, his MCS, and his PhD in Computer Science from Carleton University in Ottawa, Canada.

The Online World of the Future: Safe, Productive, and Creative

Tony Bailetti, Renaud Levesque, and D'Arcy Walsh

References

Andreasen, N. 2005. *The Creating Brain: The Neuroscience of Genius.* New York: Dana Press.

Annunziata, M. 2013. Welcome to the Age of the Industrial Internet. *TED Talks.* October 1, 2014: http://www.ted.com/talks/marco_annunziata_welcome_to_the_age_of_the_industrial_internet/

Boden, M. A. 1994. Précis of *The Creative Mind: Myths and Mechanisms. Behavioral and Brain Sciences,* 17(3): 519-570. http://dx.doi.org/10.1017/S0140525X0003569X

Boden, M. A. 1999. Computer Models of Creativity. In R. J. Sternberg (Ed.), *Handbook of Creativity:* 351-372. Cambridge: Cambridge University Press.

Cisco Systems. 2014. Internet of Everything. *Cisco Systems.* October 1, 2014: http://www.cisco.com/web/about/ac79/innov/IoE.html

Craigen, D., Walsh, D., & Whyte, D. 2013. Securing Canada's Information-Technology Infrastructure: Context, Principles, and Focus Areas of Cybersecurity Research. *Technology Innovation Management Review,* 3(7): 12-19. http://timreview.ca/article/704

Csikszentmihalyi, M. 1996. *Creativity: Flow and the Psychology of Discovery and Invention.* New York: Harper Collins.

Dubitzsky, W., Tobias K., Schmidt, O., & Berthold, M.R. 2012. Towards Creative Information Exploration Based on Koestler's Concept of Bisociation. In M. R. Berthold (Ed.), *Bisociative Knowledge Discovery:* 11-32. Berlin: Springer.

Duxbury, T. 2012. Creativity: Linking Theory and Practice for Entrepreneurs. *Technology Innovation Management Review,* 2(8): 10-15. http://timreview.ca/article/594

Gerstein, J. 2014. Addressing Maslow's Hierarchy of Needs with Technology. *User Generated Education.* October 1, 2014: http://usergeneratededucation.wordpress.com/2014/03/12/addressing-maslows-hierachy-of-needs-with-technology

Gilovich, T., Griffin, D., & Kahneman, D. 2002. *The Psychology of Intuitive Judgment.* Cambridge: Cambridge University Press.

Kahneman, D. 2011. *Thinking Fast and Slow.* Toronto: Doubleday Canada.

Koestler, A. 1964. *The Act of Creation.* New York: Penguin Books.

Leveson, N. 2013. *Engineering a Safer World.* Cambridge, MA: MIT Press.

Tibbs, H. 2013. *The Global Cyber Game: The Defence Academy Cyber Inquiry Report.* Swindon, UK: Defence Academy of the United Kingdom.

Wikipedia. 2014. The Internet of Things. *Wikipedia.* October 1, 2014: http://en.wikipedia.org/wiki/Internet_of_Things

Citation: Bailetti, T., Levesque, R., & Walsh, D. 2014. The Online World of the Future: Safe, Productive, and Creative. *Technology Innovation Management Review,* 4(10): 5–12. http://timreview.ca/article/834

Keywords: future vision, online, Internet, Internet of Things, Industrial Internet, Internet of Everything, safety, security, cybersecurity, productivity, excludability, rivalry, bisociation

Defining Cybersecurity

Dan Craigen, Nadia Diakun-Thibault, and Randy Purse

> *"To choose a definition is to plead a cause."*
>
> Charles Leslie Stevenson (1908–1979)
> Analytic philosopher

Cybersecurity is a broadly used term, whose definitions are highly variable, often subjective, and at times, uninformative. The absence of a concise, broadly acceptable definition that captures the multidimensionality of cybersecurity impedes technological and scientific advances by reinforcing the predominantly technical view of cybersecurity while separating disciplines that should be acting in concert to resolve complex cybersecurity challenges. In conjunction with an in-depth literature review, we led multiple discussions on cybersecurity with a diverse group of practitioners, academics, and graduate students to examine multiple perspectives of what should be included in a definition of cybersecurity. In this article, we propose a resulting new definition: "Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights." Articulating a concise, inclusive, meaningful, and unifying definition will enable an enhanced and enriched focus on interdisciplinary cybersecurity dialectics and thereby will influence the approaches of academia, industry, and government and non-governmental organizations to cybersecurity challenges.

Introduction

The term "cybersecurity" has been the subject of academic and popular literature that has largely viewed the topic from a particular perspective. Based on the literature review described in this article, we found that the term is used broadly and its definitions are highly variable, context-bound, often subjective, and, at times, uninformative. There is a paucity of literature on what the term actually means and how it is situated within various contexts. The absence of a concise, broadly acceptable definition that captures the multidimensionality of cybersecurity potentially impedes technological and scientific advances by reinforcing the predominantly technical view of cybersecurity while separating disciplines that should be acting in concert to resolve complex cybersecurity challenges. For example, there is a spectrum of technical solutions that support cybersecurity. However, these solutions alone do not solve the problem; there are numerous examples and considerable scholarly work that demonstrate the challenges related to organizational, economic, social, political, and other human dimensions that are inextricably tied to cybersecurity efforts (e.g., Goodall et al., 2009; Buckland et al., 2010; Deibert, 2012). Fredrick Chang (2012), former Director of Research at the National Security Agency in the United States discusses the interdisciplinary nature of cybersecurity:

"A science of cybersecurity offers many opportunities for advances based on a multidisciplinary approach, because, after all, cybersecurity is fundamentally about an adversarial engagement. Humans must defend machines that are attacked by other humans using machines. So, in addition to the critical traditional fields of computer science, electrical engineering, and mathematics, perspectives from other fields are needed."

In attempting to arrive at a more broadly acceptable definition aligned with the true interdisciplinary nature of cybersecurity, we reviewed relevant literature to identify the range of definitions, to discern dominant themes, and to distinguish aspects of cybersecurity. This research was augmented by multiple engagements with a multidisciplinary group of cybersecurity practi-

Defining Cybersecurity

Dan Craigen, Nadia Diakun-Thibault, and Randy Purse

tioners, academics, and graduate students. Together, these two activities resulted in a new, more inclusive, and unifying definition of cybersecurity that will hopefully enable an enhanced and enriched focus on interdisciplinary cybersecurity dialectics and thereby influence the approaches of academia, industry, and government and non-government organizations to cybersecurity challenges. This article reflects the process used to develop a more holistic definition that better situates cybersecurity as an interdisciplinary activity, consciously stepping back from the predominant technical view by integrating multiple perspectives.

Literature Review

Our literature review spanned a wide scope of sources, including a broad range of academic disciplines including: computer science, engineering, political studies, psychology, security studies, management, education, and sociology. The most common disciplines covered in our literature review are engineering, technology, computer science, and security and defence. But, to a much lesser extent, there was also evidence of the topic of cybersecurity in journals related to policy development, law, healthcare, public administration, accounting, management, sociology, psychology, and education.

Cavelty (2010) notes there are multiple interlocking discourses around the field of cybersecurity. Deconstructing the term cybersecurity helps to situate the discussion within both domains of "cyber" and "security" and reveals some of the legacy issues. “Cyber” is a prefix connoting cyberspace and refers to electronic communication networks and virtual reality (Oxford, 2014). It evolved from the term "cybernetics", which referred to the “field of control and communication theory, whether in machine or in the animal” (Wiener, 1948). The term "cyberspace" was popularized by William Gibson’s 1984 novel, *Neuromancer*, in which he describes his vision of a three-dimensional space of pure information, moving between computer and computer clusters where people are generators and users of the information (Kizza, 2011). What we now know as cyberspace was intended and designed as an information environment (Singer & Friedman, 2013), and there is an expanded appreciation of cyberspace today. For example, Public Safety Canada (2010) defines cyberspace as “the electronic world created by interconnected networks of information technology and the information on those networks. It is a global commons where… people are linked together to exchange ideas, services and friendship.” Cyberspace is not static; it is a dynamic, evolving, multilevel ecosystem of physical infrastructure, software, regulations, ideas, innovations, and interactions influenced by an expanding population of contributors (Deibert & Rohozinski, 2010), who represent the range of human intentions.

As for the term "security", in the literature we reviewed, there appeared to be no broadly accepted concept, and the term has been notoriously hard to define in the general sense (Friedman & West, 2010; Cavelty, 2008). According to Buzan, Wæver, and Wilde (1998), discourses in security necessarily include and seek to understand who securitizes, on what issues (threats), for whom (the referent object), why, with what results, and under what conditions (the structure). Although there are more concrete forms of security (e.g., the physical properties, human properties, information system properties, or mathematical definitions for various kinds of security), the term takes on meaning based on one’s perspective and what one values. It remains a contested term, but a central tenet of security is being free from danger or threat (Oxford, 2014). Further, although we have indicated that security is a contested topic, Baldwin (1997) states that one cannot use this designation as “an excuse for not formulating one’s own conception of security as clearly and precisely as possible”.

As a result of our literature review, we selected nine definitions of cybersecurity that we felt provided the material perspectives of cybersecurity:

1. “Cybersecurity consists largely of defensive methods used to detect and thwart would-be intruders.” (Kemmerer, 2003)

2. “Cybersecurity entails the safeguarding of computer networks and the information they contain from penetration and from malicious damage or disruption.” (Lewis, 2006)

3. “Cyber Security involves reducing the risk of malicious attack to software, computers and networks. This includes tools used to detect break-ins, stop viruses, block malicious access, enforce authentication, enable encrypted communications, and on and on.” (Amoroso, 2006)

4. “Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.” (ITU, 2009)

Defining Cybersecurity

Dan Craigen, Nadia Diakun-Thibault, and Randy Purse

5. "The ability to protect or defend the use of cyberspace from cyber-attacks." (CNSS, 2010)

6. "The body of technologies, processes, practices and response and mitigation measures designed to protect networks, computers, programs and data from attack, damage or unauthorized access so as to ensure confidentiality, integrity and availability." (Public Safety Canada, 2014)

7. "The art of ensuring the existence and continuity of the information society of a nation, guaranteeing and protecting, in Cyberspace, its information, assets and critical infrastructure." (Canongia & Mandarino, 2014)

8. "The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this." (Oxford University Press, 2014)

9. "The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation." (DHS, 2014)

Although some of these definitions include references to non-technical activities and human interactions, they demonstrate the predominance of the technical perspective within the literature. As stated by Cavelty (2010), the discourse and research in cybersecurity "necessarily shifts to contexts and conditions that determine the process by which key actors subjectively arrive at a shared understanding of how to conceptualize and ultimately respond to a security threat". Accordingly, within their particular context, the definitions above are helpful but do not necessarily provide a holistic view that supports interdisciplinarity. Referring back to Buzan, Wæver, and Wilde's (1998) discussion of securitization studies, any definition should be able to capture an understanding of the actor, subject, the referent object, the intentions and purposes, the outcomes, and structure. In our review of the literature, we did not find a definition that is inclusive, impactful, and unifying. Cybersecurity is a complex challenge requiring interdisciplinary reasoning; hence, any resulting definition must attract currently disparate cybersecurity stakeholders, while being unbiased, meaningful, and fundamentally useful.

Towards a New Definition

Faced with many definitions of cybersecurity from the literature, we opted for a pragmatic qualitative research approach to support the definitional process, which melds objective qualitative research with subjective qualitative research (Cooper, 2013). In effect, the result is a notional definition that is grounded in objectivity (e.g., an intrusion-detection system) versus supposition (e.g., the intentions of a hacker). This definitional process included: a review of the literature, the identification of dominant themes and distinguishing aspects, and the development of a working definition. This definition was in turn introduced to the multidisciplinary group discussions for further exploration, expansion, and refinement to arrive at the posited definition.

Dominant themes

In our literature review, we identified five dominant themes of cybersecurity: i) technological solutions; ii) events; iii) strategies, processes, and methods; iv) human engagement; and v) referent objects (of security). Not only do these themes support the interdisciplinary nature of cybersecurity, but, in our view, help to provide critical context to the definitional process.

Distinguishing aspects

In conjunction with the emergence of the themes, we formulated distinguishing aspects of cybersecurity, initially through discussion amongst the authors to be refined later through the multidisciplinary group discussions. In the end, we identified that cybersecurity is distinguished by:

- its interdisciplinary socio-technical character
- being a scale-free network, in which the capabilities of network actors are potentially broadly similar
- high degrees of change, connectedness, and speed of interaction

Through the process, there was consensus within the multidisciplinary group to adopt the view that the Internet is a scale-free network (e.g., Barabási & Albert, 1999), meaning it is a network whose degree distribution follows a power law, at least asymptotically. Even though this characterization of the Internet is a subject of debate (e.g., Wallinger et al., 2009), we argue that there are cyber-attack scenarios, and especially the evolution of malware markets, where the capabilities

Defining Cybersecurity

Dan Craigen, Nadia Diakun-Thibault, and Randy Purse

for launching attacks has been largely commoditized, hence flattening the space of network actors.

Throughout the initial part of the process that resulted in a working paper, we intentionally attempted to redress the technical bias of extant definitions in the cybersecurity literature by ensuring that scholars and practitioners contributed to the discussion and were provided an opportunity to review and comment on our initial definition, themes, and distinguishing aspects. To expand the discussion and create additional scholarly dialogue, we posited an original "seed" definition for discussion and further refinement during two three-hour engagements with a multidisciplinary group of cybersecurity practitioners, academics, industry experts from the VENUS Cybersecurity Institute (venus cyber.com), and graduate students in the Technology Innovation Management program (timprogram.ca) at Carleton University in Ottawa, Canada.

Emergent definitions of cybersecurity

Our engagement with the multidisciplinary group primarily consisted of providing selected readings from the literature, an initial presentation and discussion of our own work to date, followed by a syndicate activity related to distinguishing aspects and defining cybersecurity. Three syndicates were formed from the group and they were asked to develop their own definitions. These definitions, along with the authors' brief critiques, are presented in Table 1. The first two definitions were developed by the authors, whereas the next three definitions arose from group participants.

Table 1. Emergent cybersecurity definitions and critiques

	Participant Working Definitions	Critique(s)
1	"Cybersecurity is the protection of information/data, assets, services, and systems of value to reduce the probability of loss, damage/corruption, compromise, or misuse to a level commensurate with the value assigned."	In the main, the feedback suggested that the inclusion of value introduced the human concepts related to security, but that the definition was too prescriptive and suffered the problem of a restrictive "listing" of what is being protected.
2	"Cybersecurity is a collection of interacting processes intended to protect cyberspace and cyberspace-enabled systems (collectively resources) from intentional actions designed to misalign actual resource property rights from the resource owner perceived property rights."	This definition introduced the emerging cyber-physical environment and included the important concept of control over property rights. However, the definition's focus on "human intentional actions" was viewed as being overly restrictive.
3	"Cybersecurity is a collection of interacting processes intended to make cyberspace safe and secure."	Specifically intended to be broader than the seed definition, this definition introduced more problems than it solved because it was unnecessarily broad and introduced the contested notion of safety with security.
4	"Cybersecurity is a domain dedicated to the study and practice of the protection of systems or digital assets from any action taken to impose authorization on those systems or digital assets that do not align with the property rights of the resource facility as understood by its owner."	In this definition, the concepts of property rights and control were introduced. However, there were concerns about the potential implications of "action taken" to mean limiting cybersecurity to human actors. Also there were concerns regarding the terms, which imposed limits on the scope of the definition such as "study" and "practice", thereby situating the issues largely within the academic domain.
5	"Cybersecurity is the state in which power over the execution of computers (sensu lato) and over information in the control of computers is where it should be."	This definition reinforced the notions of control over information and systems. The main criticism was defining cybersecurity as a state.

Defining Cybersecurity

Dan Craigen, Nadia Diakun-Thibault, and Randy Purse

A New Definition of Cybersecurity

We propose the following definition, which integrates key concepts drawn from the literature and engagement with the multidisciplinary group:

Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure *from* de facto *property rights.*

We deconstruct this definition as follows:

- *…the organization and collection of resources, processes, and structures…*: This aspect captures the multiple, interwoven dimensions and inherent complexity of cybersecurity, which ostensibly involve interactions between humans, between systems, and between humans and systems. By avoiding discussion of which resources, processes, or structures, the definition becomes non-prescriptive and recognizes the dynamic nature of cybersecurity.

- *…used to protect cyberspace and cyberspace-enabled systems…*: This aspect includes protection, in the broadest sense, from all threats, including intentional, accidental, and natural hazards. This aspect also incorporates the traditional view of cyberspace but includes those systems that are not traditionally viewed as part of cyberspace, such as computer control systems and cyber-physical systems. By extension, the protection applies to assets and information of concern within cyberspace and connected systems.

- *…from occurrences…*: This aspect recognizes that "protections" are intended to address the full range of intentional events, accidental events, and natural hazards. It also suggests that some of the occurrences are unpredictable.

- *…that misalign* de jure *from* de facto *property rights…*: This aspect incorporates the two separate notions of ownership and control that dominate discussion of cybersecurity and digital assets introduced in the property rights framework of Ostrom and Hess (2007), which include access, extraction, contribution, removal, management, exclusion, and alienation. Any event or activity that misaligns actual (*de facto*) property rights from perceived (*de jure*) property rights, whether by intention or accident, whether known or unknown, is a cybersecurity incident.

Substantiating Our Definition

As discussed earlier, our definition should engender greater interdisciplinary and collaborative efforts on cybersecurity. Our goal is to "bring together" not to "push apart" or "isolate". Our success (or failure) can be partly validated if we can demonstrate that:

1. We can map other definitions of cybersecurity into our definition.

2. Our definition is unifying and inclusive in that it supports interdisciplinarity.

To assist in the analysis and mapping of the definitions to our new definition, we identified conceptual categories from definitions drawn from the literature as well as our own definition (Table 2). Unless otherwise cited, the category definitions are drawn largely from the Oxford (2014) online dictionary. The exact wordings of the definitions are meant to be as encompassing as possible.

A number of definitions of cybersecurity were presented in this article. Some of the definitions are from the literature and drive the perspectives of certain communities. Other definitions arose through our group discussions and related activities. Table 3 provides examples of how our analysis was applied to sample definitions from the literature and group discussions.

The above analysis helps to demonstrate that our new definition is inclusive of key components from a sample of extant and participant definitions. Furthermore, three of the dominant themes – technological solutions; strategies, processes, and methods; and human engagement – are all refinements of the "the organization and collection of resources, processes, and structures used to protect..." component of our definition. The dominant theme of "events" is a refinement of "occurrences." We also view "referent objects (of security)" as a refinement of "cyberspace and cyberspace-enabled systems." Retrospectively, we therefore show how our definition is consistent with the dominant themes of cybersecurity and reflects the previously identified distinguishing aspects. Therefore, this mapping illustrates how our definition supports interdisciplinarity.

Conclusion

We have provided a new, more inclusive, and unifying definition of cybersecurity that we believe will enable an enhanced and enriched focus on interdisciplinary cy-

Defining Cybersecurity

Dan Craigen, Nadia Diakun-Thibault, and Randy Purse

bersecurity dialectics and, thereby, will influence the approaches of researchers, funding agencies, and organizations to cybersecurity challenges. For example, the new definition and associated perspectives could lead to changes in public policy and inform legislative actions.

The definition resulting from the work reported herein has a number of potentially salutary features, including:

1. Contributing a major unifying theme by positioning cybersecurity as an interdisciplinary domain, not a technical domain.

2. Supporting inclusiveness demonstrated through the relationship to the five dominant cybersecurity themes and mapping to previous definitions.

3. Incorporating the evolution towards a more interconnected world through inclusion of both cyberspace and cyberspace-enabled systems. The latter includes cyber-physical systems and control systems.

4. Using protection – as a fundamental concept within security – in a broad sense within the definition, including protection from intentional events, accidental events, and natural hazards.

5. Incorporating the "property rights" framework of Ostrom and Hess (2007), which includes access, extraction, contribution, removal, management, exclusion, and alienation. Thus, the discussion moves beyond traditional assets and information terms to broadly include that which has meaning or value.

The absence of a concise, universally acceptable definition that captures the multidimensionality of cybersecurity impedes technological and scientific advances by reinforcing the predominantly technical view of cybersecurity while separating disciplines that should be acting in concert to resolve complex cybersecurity challenges. It has become increasingly apparent that cybersecurity is interdisciplinary. The more inclusive, unifying definition presented in this article aims to facilitate interdisciplinary approaches to cybersecurity. We hope that the definition will be embraced by the multiple disciplines engaged in cybersecurity efforts, thereby opening the door to greater understanding and collaboration needed to address the growing and complex threats to cyberspace and cyberspace-enabled systems.

Table 2. Conceptual categories and their definitions

Category	Definition
Asset	In general, defined as "a useful or valuable thing or person". Here, we refine the definition to refer to "cyberspace and cyberspace-enabled systems".
Capability	An abbreviation for the organization and combination of resources, processes, and structures.
Misalign	Align is defined as "put (things) into correct appropriate relative positions"; hence, misalign results in incorrect or inappropriate positions.
Occurrence	An incident or event.
Organization	"A firm's policies and procedures 'organized to exploit the full competitive potential of its resources and capabilities'" (Kozlenkova et al., 2013). We generalize "firms" to "institutions".
Process	The fact of going on or being carried on, as a action or series of actions; progress, course. *in (the) process of (doing something):* in the course of; in the act of carrying out (a particular task, etc.). *in process:* going on, being done; in progress
Property right	An enforceable authority to undertake particular actions in specific domains. Includes the rights of access, withdrawal, management, exclusion, and alienation (Ostrom & Hess, 2007).
Protect	Keep safe from harm or injury.
Resource	"Tangible and intangible assets ['firms'] use to conceive of and implement [their] strategies" (Kozlenkova et al., 2013). We generalize "firms" to "institutions".

Defining Cybersecurity

Dan Craigen, Nadia Diakun-Thibault, and Randy Purse

Table 3. Examples of cybersecurity definitions and related analysis of the proposed definition

Definitions of Cybersecurity	**Analysis** (Key Terms → Corresponding Terms in Proposed Definition)
"The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this." (Oxford University Press, 2014)	"protected" → PROTECT "criminal or unauthorized use" → MISALIGN "electronic data" → ASSETS and PROPERTY RIGHTS "measures taken..."→ CAPABILITY
"The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation." (DHS, 2014)	"activity or process, ability or capability, or state" → CAPABILITY " information and communications systems and the information contained therein" → ASSETS and PROPERTY RIGHTS "protected from and/or defended" → PROTECT "damage, unauthorized use or modification, or exploitation" → MISALIGN
"Cybersecurity entails the safeguarding of computer networks and the information they contain from penetration and from malicious damage or disruption." (Lewis, 2006)	"safeguarding" → CAPABILITY "computer networks and information" → ASSETS and PROPERTY RIGHTS "penetration and from malicious damage or disruption" → OCCURRENCES or MISALIGN
"Cybersecurity involves reducing the risk of malicious attack to software, computers and networks. This includes tools used to detect break-ins, stop viruses, block malicious access, enforce authentication, enable encrypted communications, and on and on." (Amoroso, 2006).	"involves reducing the risk" → CAPABILITY "of malicious attack" → OCCURRENCES or MISALIGN "software, computers and networks" → ASSETS and PROPERTY RIGHTS "includes tools used to detect break-ins, stop viruses, block malicious access, enforce authentication, enable encrypted communications, and on and on" → CAPABILITY
"Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets." (ITU, 2009)	"the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies" → CAPABILITY "to protect" → PROTECT "cyber environment and organization and user's assets" → ASSETS and PROPERTY RIGHTS
"Cybersecurity is a collection of interacting processes intended to make cyberspace safe and secure." (Definition from group discussions)	"interacting processes" → PROCESS and CAPABILITY "safe and secure" → PROTECT
"Cybersecurity is the state in which power over the execution of computers (sensu lato) and over information in the control of computers is where it should be." (Definition from group discussions)	"power over the execution of computers and over information in the controls of computers is where it should be"→ ASSETS and PROPERTY RIGHTS

Defining Cybersecurity

Dan Craigen, Nadia Diakun-Thibault, and Randy Purse

About the Authors

Dan Craigen is a Science Advisor at the Communications Security Establishment in 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 in Ottawa, Canada.

Nadia Diakun-Thibault is Senior Science and Analytics Advisor at the Communications Security Establishment in Canada. She holds a Master's degree in Public Administration from Queen's University in Kingston, Canada, and an ABD (PhD) degree in Slavic Languages and Literatures from the University of Toronto, Canada. She has served as Parliamentary Advisor to Members of Parliament and held an Order-in-Council appointment to the Province of Ontario's Advocacy Commission. Her research interests include neurophilosophy, semiotics, linguistics, and public policy. She is also an adjunct faculty member in the Department of Computer Science and Engineering at North Carolina State University in the United States.

Randy Purse is the Senior Learning Advisor at the Information Technology Security Learning Centre at the Communications Security Establishment in Canada. A former officer in the Canadian Forces, he is an experienced security practitioner and learning specialist. His research interests include the human dimensions of security and collective and transformative learning in the workplace. He has a Master's of Education in Information Technology from Memorial University of Newfoundland in St. John's, Canada, and he is a PhD candidate specializing in Adult and Workplace Learning in the Faculty of Education at the University of Ottawa, Canada.

Acknowledgements

The authors wish to thank Tony Bailetti, George Cybenko, George Dinolt, Risto Rajala, and Mika Westerlund for reviewing and commenting on an earlier draft of this article. We also wish to thank the participants in the multidisciplinary group for their informed engagement.

References

Amoroso, E. 2006. *Cyber Security.* New Jersey: Silicon Press.

Baldwin, D. A. 1997. The Concept of Security. *Review of International Studies,* 23(1): 5-26.

Barabási, A. L., & Albert, R. 1999. Emergence of Scaling in Random Networks. *Science,* 286(5439): 509-512. http://dx.doi.org/10.1126/science.286.5439.509

Buzan, B., Wæver, O., & De Wilde, J. 1998. *Security: A New Framework for Analysis.* Boulder, CO: Lynne Rienner Publishers.

Canongia, C., & Mandarino, R. 2014. Cybersecurity: The New Challenge of the Information Society. In *Crisis Management: Concepts, Methodologies, Tools and Applications:* 60-80. Hershey, PA: IGI Global. http://dx.doi.org/10.4018/978-1-4666-4707-7.ch003

Cavelty, M. D. 2008. Cyber-Terror—Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate. *Journal of Information Technology & Politics,* 4(1): 19-36. http://dx.doi.org/10.1300/J516v04n01_03

Cavelty, M. D. 2010. Cyber-Security. In J. P. Burgess (Ed.), *The Routledge Handbook of New Security Studies:* 154-162. London: Routledge.

Chang, F. R. 2012. Guest Editor's Column. *The Next Wave,* 19(4): 1–2.

CNSS. 2010. National Information Assurance Glossary. Committee on National Security Systems (CNSS) Instruction No. 4009: http://www.ncix.gov/publications/policy/docs/CNSSI_4009.pdf

Cooper, S. 2013. Pragmatic Qualitative Research. In M. Savin-Baden & C. H. Major (Eds.), *Qualitative Research: The Essential Guide to Theory and Practice:* 170-181. London: Routledge.

Deibert, R., & Rohozinski, R. 2010. Liberation vs. Control: The Future of Cyberspace. *Journal of Democracy,* 21(4): 43-57. http://dx.doi.org/10.1353/jod.2010.0010

DHS. 2014. A Glossary of Common Cybersecurity Terminology. National Initiative for Cybersecurity Careers and Studies: Department of Homeland Security. October 1, 2014: http://niccs.us-cert.gov/glossary#letter_c

Friedman, A. A., & West, D. M. 2010. Privacy and Security in Cloud Computing. *Issues in Technology Innovation,* 3: 1-13.

Goodall, J. R., Lutters, W. G., & Komlodi, A. 2009. Developing Expertise for Network Intrusion Detection. *Information Technology & People,* 22(2): 92-108. http://dx.doi.org/10.1108/09593840910962186

ITU. 2009. Overview of Cybersecurity. Recommendation ITU-T X.1205. Geneva: International Telecommunication Union (ITU). http://www.itu.int/rec/T-REC-X.1205-200804-I/en

Kozlenkova, I. V., Samaha, S. A., & Palmatier, R. W. 2014. Resource-Based Theory in Marketing. *Journal of Academic Marketing Science,* 42(1): 1-21. http://dx.doi.org/10.1007/s11747-013-0336-7

Kemmerer, R. A. 2003. *Cybersecurity. Proceedings of the 25th IEEE International Conference on Software Engineering:* 705-715. http://dx.doi.org/10.1109/ICSE.2003.1201257

Lewis, J. A. 2006. *Cybersecurity and Critical Infrastructure Protection.* Washington, DC: Center for Strategic and International Studies. http://csis.org/publication/cybersecurity-and-critical-infrastructure-protection

Defining Cybersecurity

Dan Craigen, Nadia Diakun-Thibault, and Randy Purse

Ostrom, E., & Hess, C. 2007. Private and Common Property Rights. In B. Bouckaert (Ed.), *Encyclopedia of Law & Economics*. Northampton, MA: Edward Elgar.

Oxford University Press. 2014. *Oxford Online Dictionary*. Oxford: Oxford University Press. October 1, 2014: http://www.oxforddictionaries.com/definition/english/Cybersecurity

Public Safety Canada. 2010. *Canada's Cyber Security Strategy*. Ottawa: Public Safety Canada, Government of Canada. http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-eng.aspx

Singer, P. W., & Friedman, A. 2013. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York: Oxford University Press.

Public Safety Canada. 2014. *Terminology Bulletin 281: Emergency Management Vocabulary*. Ottawa: Translation Bureau, Government of Canada. http://www.bt-tb.tpsgc-pwgsc.gc.ca/publications/documents/urgence-emergency.pdf

Wallinger, W., Alderson, D., & Doyle, J. 2009. Mathematics and the Internet: A Source of Enormous Confusion and Great Potential. *Notices of the American Mathematical Society,* 56(5): 586-599.

Citation: Craigen, D., Diakun-Thibault, N., & Purse, R. 2014. Defining Cybersecurity. *Technology Innovation Management Review*, 4(10): 13–21. http://timreview.ca/article/835

Keywords: cybersecurity, definition, interdisciplinary, cyberspace, security

Effective Digital Channel Marketing for Cybersecurity Solutions

Mika Westerlund and Risto Rajala

> *"Why kick the man downstream who can't put the parts together because the parts really weren't designed properly?"*
>
> Philip Caldwell (1920–2013)
> Former CEO of the Ford Motor Company

Smaller organizations are prime targets for hackers and malware, because these businesses lack cybersecurity plans and the resources to survive a serious security incident. To exploit this market opportunity, cybersecurity solution providers need to leverage the power of downstream channel members. We investigate how a supplier's digital channel marketing can encourage value-added resellers to sell that supplier's cybersecurity solutions. Our analysis of survey data from 109 value-added resellers of a multinational supplier shows that resellers are more committed to stock and sell cybersecurity products and services if the supplier's digital channel marketing provides tools that help them sell the solutions to end customers. This support is likely needed because cybersecurity offerings are technologically complex and systemic by nature, as supported by the finding that value-added resellers pay little attention to supplier's campaigns and price discounts. Thus, cybersecurity suppliers should maintain trusted and informative relationships with their resellers and provide them with hands-on sales tools, because a reseller's commitment to selling cybersecurity solutions is linked with their ability to understand the offering and with the extent of their supplier relationship. These findings are in line with previous literature on the challenges perceived by salespeople in selling novel and complex technology.

Introduction

According to The 2112 Group (2014), the volume and severity of cyber-threats and malware represent the second highest operational risk for small and midsized businesses, behind only economic uncertainty. Yet, four out of five such businesses have no cybersecurity plans, meaning there is a substantial market opportunity for cybersecurity providers. One of the most effective ways to reach these numerous potential customers is to leverage the power of downstream channels (cf. Sreenivas & Srinivas, 2008; Chung et al., 2012). Value-added resellers are systems integrators that can work either with a single vendor that offers most of the technology needed to build end-to-end offerings, or multiple vendors to integrate and craft more comprehensive solutions. Although many value-added resellers prefer working with a single vendor, a growing number show better returns by creating holistic solutions using multiple "best-of-breed" technologies (The 2012 Group, 2014). Given that value-added resellers have choices in sourcing, assembling, and deploying hardware and software solutions for customers, cybersecurity suppliers need to build brand awareness to maximize the popularity of their products as a part of the reseller's total solutions.

Digitization has redefined how contemporary businesses communicate across their channels of distribution (Rapp et al., 2013). Holden-Bache (2011) refers to a study by BtoB Magazine in which more than 93 percent of business-to-business marketers were found to use

Effective Digital Channel Marketing for Cybersecurity Solutions

Mika Westerlund and Risto Rajala

one or more forms of social media to interact with their downstream channel members. According to Kalyanam and Brar (2009), designing a channel-management system that enables value-added resellers to sell solutions to end users is an important strategy, particularly in the information and communication technology industry. Furthermore, Jerman and Zavrsnik (2012) suggest that the success of an organization can result from the effectiveness of its marketing communication. Hence, a firm should have a business model that tracks how marketing communication influences what its customers know, believe, and feel, and how they behave.

Much of the current research on downstream channel marketing focuses on value propositions associated with products or services. In addition, many studies on marketing communications have focused on the consumer market, with little regard for the business-to-business market (Jerman & Zavrsnik, 2012). The determinants of perceived value associated with complex products and services, such as cybersecurity, remain unclear and largely under-explored (Menon et al., 2005). Hence, the existing literature offers limited empirical and theoretical insight into marketing communications effectiveness in business-to-business marketing. Specifically, there is little help for marketing managers when planning effective communications strategies and understanding the impact of their suppliers' channel marketing activities (Jerman & Zavrsnik, 2012).

To address these gaps in the literature, we investigate the effectiveness of digital channel marketing in the context of business-to-business cybersecurity solutions. We consider that cybersecurity is an interesting context given the growing demand for cybersecurity solutions, especially among small and midsized businesses, and acknowledge that the marketing activities of suppliers in downstream channels are increasingly digital by nature. Craigen and colleagues (2014) define cybersecurity as "the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign *de jure* from *de facto* property rights." Bearing this definition in mind, our study aims to improve the current understanding of how cybersecurity solution providers can increase the impact of their digital channel marketing by focusing on the paramount marketing activities and by allocating their marketing resources accordingly. Further, our study draws on the view of Johanson (2013), who defines cybersecurity products as software, hardware, and services that help users protect themselves from cybersecurity threats related to information sharing, security risks, cyber-incidents, and cybercrime, as well as cyber-intrusions. Thus, we investigate cybersecurity solutions as the offerings consisting of products and related expertise provided to meet the customers' cybersecurity needs and posit a research question: How can suppliers of cybersecurity solutions use digital channel marketing effectively to promote their products in the downstream channel?

To answer our research question, we investigate the effects of digital channel marketing by cybersecurity solution providers in terms of its functional, informative, and relational qualities, as well as the influence of marketing abundance on the effectiveness of digital channel marketing by cybersecurity solution providers. According to Kalyanam and Brar (2009), there are many ways in which channel partners such as resellers can help generate demand. Resellers are often deeply embedded in the customer's decision-making processes and are able to create and offer solutions to customer's specific business situation and technology needs. Thus, suppliers need to focus on creating top-of-mind awareness among their value-added resellers to ensure them becoming a preferred supplier when resellers are in a position to sell cybersecurity solutions to the end customers.

The article is structured as follows. After this introduction, we discuss the objectives and activities of digital channel marketing on the basis of prior literature. Then, we present our research model and methodological approach. Thereafter, we present the results, limitations, and future research opportunities regarding our empirical inquiry. We conclude by discussing the implications for research and practice.

Digital Channel Marketing

A supplier's success in the marketplace is at least partly contingent on their ability to energize downstream channel members to resell their products and services, according to Hughes and Ahearne (2010). Moreover, Danaher and Rossiter (2011) argue that digital marketing communication is a vital part of the relationship between a supplier and a value-added reseller. Contemporary marketers face an increasingly wide and diverse choice of digital media channels through which they aim to energize their brokers, agents, wholesalers, and retailers to sell their products and services effectively to other channel members, and, ultimately, to the end

Effective Digital Channel Marketing for Cybersecurity Solutions

Mika Westerlund and Risto Rajala

users. As Internet technologies have become an everyday part of the workplace for millions of people around the globe, current marketing channels feature many digital elements such as banner ads, email and blogs, social software, and text messaging (SMS). Lindgreen and colleagues (2006) show that many suppliers increasingly use digital communications to interact with their resellers rather than face-to-face interaction.

To be effective, channel marketing communications should create value for channel partners. According to Simpson, Siguaw, and Baker (2001), the objective of creating value for channel partners and the desire to capture part of that value are the reasons suppliers enter into relationships with value-added resellers. Barry and Terry (2008) point out that the determinants of value have an economic, technical, and functional dimension. Economic value refers to pricing (how much something costs), while technical value points to deliverables (what is received) and functional value refers to delivery (how it is received). Payne and Holt (2001) argue that, according to the augmented product view, competition between companies is not based solely on products and services, but also on advertising and customer advice that create value for the downstream channel members. Edwards, Battisti, and Neely (2004) anticipate that the benefits of digital channel marketing for value-added resellers depend upon the quality and extent of activities the supplier generates through digital marketing. The benefits of digital channel marketing may be realized by communicating the value of factors beyond the core product or service (Lilien et al., 2010).

The effectiveness of marketing communications can be measured in several ways, although in terms of economic measures, the most common indicator of marketing performance is the volume of sales. Danaher and Rossiter (2011) investigate supplier-initiated marketing communication and measure the effect of promotional offers in an electronic medium on intentional customer behaviour. Thus, marketing effectiveness in supply chains can be measured as the reseller's intention and increased efforts to sell a supplier's products and services (Johnson et al., 2001). Kalyanam and Brar (2009) found that, because resellers in the dynamic information technology industry are typically selling many technologies, they lack the time to focus and learn specific technologies or product information. Following Jerman and Zavrsnik (2012), we see that it is important for marketers to understand the contribution of different marketing objectives to the overall effectiveness of their marketing communications.

Relational qualities

The relational qualities of digital channel marketing focus on strengthening the supplier's relationships with the members in the downstream channel. This notion is concordant with the thesis by Webster (2000), according to which, in the relationship between the supplier, reseller, and end customer, the quality of the relationship for any given actor will depend on the quality and strength of the relationship between the other two actors. The value of the supplier relationship, as perceived by the reseller, usually refers to the net benefits realized through the supplier's offerings or the supplier-reseller relationship (Kumar et al., 1992). It builds on the assumption that value-added resellers want to maximize the perceived benefits and minimize the perceived sacrifices (Lindgreen & Wynstra, 2005). A supplier's business marketing communications have great potential to produce such value to the value-added reseller. According to Andersen (2001), marketing communication is connected with relationship development, and the receiver's commitment to the sender is preceded by awareness and persuasion.

Relationship marketing scholars have found that communication is a fundamental aspect of relationship development – it is the glue that holds together the channel of distribution (Anderson, 2001). Andersen also notes that communication has a direct impact on central aspects of relationship marketing such as trust, coordination, and commitment. Communication is seen as an independent or mediating variable for partnership success (Mohr & Spekman, 1994). The essence of these activities is to decrease exchange uncertainty and to encourage customer collaboration and commitment through gradual development and ongoing adjustment of mutual norms and shared routines. If customers are retained over several transactions, both buyers and sellers may profit from the experience gained through previous transactions (Andersen, 2001). Accordingly, we developed the following hypothesis:

Hypothesis 1: *Digital channel marketing that strengthens the relationship between supplier and value-added reseller is positively linked with the reseller's intention to sell the supplier's cybersecurity solutions.*

Informative qualities

The informative qualities of channel marketing ensure that value-added resellers are kept up to date with campaigns and product developments. Jerman and Zavrsnik (2012) posit that marketing communications

Effective Digital Channel Marketing for Cybersecurity Solutions

Mika Westerlund and Risto Rajala

aimed at downstream channel members play more of an informational and supportive role than do those that target end consumers. Marketing communications need to provide clear, pertinent, and timely information, so that good decisions can be made (Jerman & Zavrsnik, 2012). Hansen and colleagues (2008) suggest that information sharing increases the value of the supplier-reseller relationship, as perceived by the value-added reseller, and it fosters adaptation and trust in that relationship. Moreover, Edwards, Battisti, and Neely (2004) found that suppliers can be a key source of information for buyers, exceeded only by the company's internal knowledge acquisition. Hansen, Samuelsen, and Silseth (2008) point out that suppliers may inform their value-added resellers about the product-related information relevant for the relationship, including changes in pricing, changes in market, new products and services, as well as organizational changes that may affect the supplier-reseller relationship. In particular, sales promotion is an informative type of communication that consists of a set of short-term motivational tools used to encourage buyers to buy more and promptly (Rahmani et al., 2012).

According to Kalyanam and Brar (2009), high-tech companies such as Cisco, which has invested significantly in digital channel marketing, training, and certification programs for its downstream channel members, have enjoyed increased sales volumes. Therefore, Simpson, Siguaw, and Baker (2001) argue that the supplier's activity as a provider of information can serve as a critical informational resource for the reseller. One-way oriented communication, such as advertising, branding, and other traditional tools, may help the supplier develop an attractive personality profile (Andersen, 2001). Hence, if a supplier has developed an attractive image in the mind of the prospective buyer, it may cause the decision maker to look for information on this particular supplier first: a top-of-the-mind effect (Andersen, 2001). Hence, we developed the following hypothesis:

Hypothesis 2: *Digital channel marketing that is informative of supplier's campaigns and price discounts is positively linked with the reseller's intention to sell the supplier's cybersecurity solutions.*

Functional qualities

Functionally motivated communication supports the capability of downstream channel members to resell the suppliers' products. For example, suppliers may possess specific expertise, which the downstream channel partners may not have in-house or may not want to acquire (Ulaga, 2003). This benefit is especially important with complex technology such as cybersecurity products and services. Therefore, a supplier of cybersecurity products can provide benefit to value-added resellers by educating and helping them improve their skills and competences to sell the supplier's products. Supplier-provided facilities and tools are among the key factors that augment the value perceived by downstream channel partners (Simpson et al., 2001). In addition, Simpson, Siguaw, and Baker (2001) contend that product and service related training is perceived valuable by resellers. These tools include point-of-sale scanner data for inventory, promotion and payment management, customer management database tools, and an online presence for Internet marketing. According to Simpson and colleagues (2001), research has shown that these supplier-provided tools improve the sales performance of value-added resellers. Also, Lindgreen and colleagues (2006) suggest that the value of channel marketing goes beyond the immediate value of goods or services, given that the education the supplier provides is part of that value.

We consider the functional objectives to be instrumental by nature, because the supplier helps its value-added resellers obtain something to improve their sales performance. In doing so, we comprehend the instrumental value of suppliers' digital channel marketing through two distinct aspects. First, it implies that value-added resellers perceive the digital marketing communications of their suppliers as useful, because it helps the resellers to develop and improve their selling skills and capabilities. Second, it gives the resellers new tools for selling complex products and services. Based on these notions, we consider it reasonable to suggest that digital channel marketing by suppliers can support resellers by providing them with professional skills or practical tools that improve their sales performance. Therefore, we developed the following hypothesis for the context of cybersecurity:

Hypothesis 3: *Digital channel marketing that provides functional support to resellers is positively linked with the resellers' intention to sell the supplier's cybersecurity solutions.*

Abundant digital channel marketing, sales intention, and stocking decisions

Previous research does not consistently show whether more digital marketing is better from the performance point of view. There may be a valuable premium in frequency and continuity of marketing messages to the

Effective Digital Channel Marketing for Cybersecurity Solutions

Mika Westerlund and Risto Rajala

customers. Danaher and Rossiter (2011) researched how customers perceive marketing communications and direct marketing messages they receive from suppliers in various ways, including different channels. Surprisingly, senders rate email more negatively than receivers do. That is, business receivers view email messages in a positive light, but senders are more cautious in fear of using it excessively. Thus, it makes sense, for instance, to send multiple waves of marketing emails, because marketers in the digital era cannot count on the recipients to open a particular email message. Consequently, we developed the following hypothesis:

Hypothesis 4: *Abundant digital channel marketing is positively linked with reseller's intention to sell the supplier's cybersecurity solutions.*

The theory of reasoned action developed by Fishbein and Ajzen (1975) and its successor, the theory of planned behaviour proposed by Ajzen (1985), are among the most predictive persuasion theories. They have been applied to studies of the relations among beliefs, attitudes, behavioural intentions and behaviours in various fields such as advertising, public relations, and marketing. The theory states that behavioural intention, which is a function of attitudes toward behavioural and subjective norms toward that behaviour, predict actual behaviour. Thus, we developed the following hypothesis:

Hypothesis 5: *The intention of value-added resellers to sell a supplier's cybersecurity solutions is positively linked with its stocking decisions.*

Model

Our research model is rooted in previous studies on the effectiveness of advertising on sales performance. One of them is the article by Hughes (2013) about the effects of advertisement on sales efforts and performance of resellers. Jerman and Zavrsnik (2012) confirm that marketing communications have a positive effect on the market performance of suppliers. With increasing calls for accountability of significant marketing communication spending, it is imperative to measure the contribution of marketing communication to firm performance (Jerman & Zavrsnik, 2012).

Lemmink and colleagues (1998) have proposed that customer value includes emotional, logical, and practical benefits. We amend their conceptualization for a better fit with channel marketing in supply chains, and anticipate that the supplier's digital channel marketing provides resellers with relational, informative, and functional benefits. These benefits comprise the perceived quality of digital channel marketing, whereas marketing abundance, referring to the extent and volume of marketing messages, reflects the quantity of marketing. In our research model, sales intention refers to a reseller's increased effort to sell the supplier's products and the reseller's stocking decision is understood as the actual purchase of the supplier's products to ensure its stock-and-sell availability. As the hypothesized model illustrates, we anticipate that both quality and quantity of a supplier's digital channel marketing contribute to the sales intention of its value-added resellers, and, ultimately, to their stocking decisions (Figure 1).

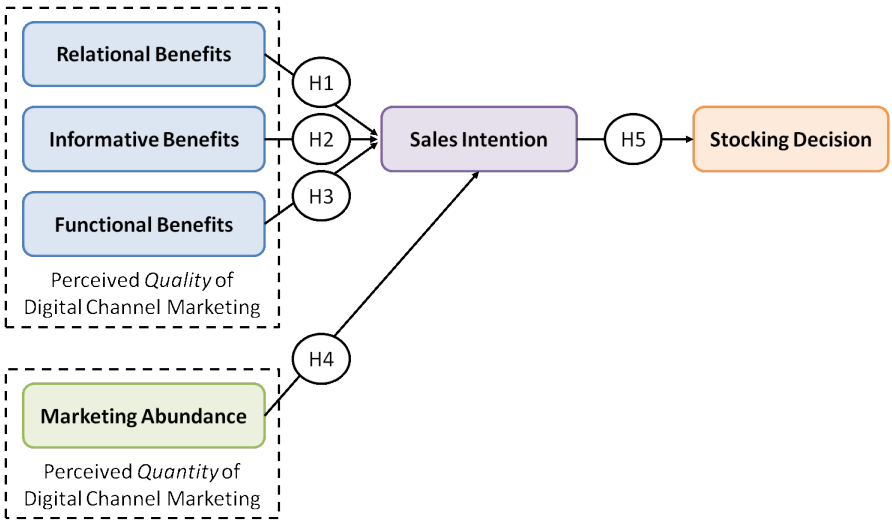

Figure 1. Research model, including the five hypotheses

Effective Digital Channel Marketing for Cybersecurity Solutions

Mika Westerlund and Risto Rajala

Methodology

We conducted an online survey in late 2008 among Finnish retailers of an internationally operating supplier of cybersecurity products. The company provides a broad range of data security, cybersecurity, and infrastructure security solutions to value-added resellers in 15 countries in Europe and North America. To select the target companies for the survey, we administered it to the active resellers of the supplier's products. Our contact at the company sent an invitation to participate in the survey to 335 potential respondents by email. The questionnaire yielded 109 usable responses, thus giving a response rate of 32.5 percent. We measured all items on a five-point Likert scale (1="strongly disagree" to 5="strongly agree).

We chose the Partial Least Squares (PLS) path-modelling method for our empirical analysis. The advantages of PLS include the ability to model multiple constructs, to explore the relative importance of the independent variables, and the ability to handle their multicollinearity. In addition, the method provides us with robustness in the face of missing data; it poses minimum requirements on measurement levels and allows the creation of independent latent variables directly on the basis of cross-products involving the response variables (Chin et al., 2003; Tenenhaus et al., 2005). These concerns are important in our research setting, where there is no strong theory to test in order to explain the phenomenon. In practice, PLS helps to avoid biased and inconsistent parameter estimates for equations, which is appropriate when the research model is in an early stage of development (Teo et al., 2003). We performed the empirical analysis using the SmartPLS 2.0 software by Ringle Wende, and Will (2005).

Results

The results of our hypothesis testing show that H1, H3, and H5 are supported, whereas H2 and H4 are not supported. In other words, the results suggest that relational benefits (H1; β=.26, p<.05) and functional benefits (H3; β=.60, p<.001) of a cybersecurity suppliers' digital channel marketing are positively linked with the increased sales intention of the value-added resellers. Moreover, this sales intention (H5; β=.42, p<.001) is positively linked with the reseller's actual stocking behaviour. On the contrary, informative benefits (H2; β=-.09, n.s.) and the quantity of marketing in terms of abundant marketing messages (H4; β=.08, n.s.) are not linked with the increased sales intension of the value-added resellers. Table 1 presents the results of hypothesis testing, and Appendix 1 discusses the details of our analysis.

Every analysis has limitations, which provide opportunities for future research. First, we discussed the quality of digital channel marketing in terms of relational, informative, and functional benefits. An in-depth review of marketing communication theory may reveal other aspects, practices, or occasions that can affect the results. Further analysis could also reveal possible differences between new and established relationships between supplies and value-added resellers regarding the impact of supplier's digital channel marketing on the behavioural sales intention of resellers (cf. Andersen, 2001). Second, because our study was conducted in one European country only and focused on cybersecurity as a specific form of complex technology, future research may test our findings in other countries or market areas and in other domains beyond cybersecurity. Third, the results may be different if the effective-

Table 1. Results of hypotheses testing (n=109, bootstrap samples=1000, df=115)

Hypothesis	Relationship	β	*t*-value	*p*-value	Support
H1	RELATIONAL → SALES INTENTION	.26	2.70	.008	Yes
H2	INFORMATIVE → SALES INTENTION	-.09	1.30	.197	No
H3	FUNCTIONAL → SALES INTENTION	.60	6.87	.000	Yes
H4	ABUNDANT → SALES INTENTION	.08	.90	.370	No
H5	SALES INTENTION → STOCK	.42	3.96	.000	Yes

Effective Digital Channel Marketing for Cybersecurity Solutions

Mika Westerlund and Risto Rajala

ness of the supplier's digital channel marketing is measured using other variables. Our analysis measured the stocking behaviour of value-added resellers in terms of subjective self-assessment. The behaviour should also be studied using objective financial and non-financial outcomes, such as actual sales figures, purchase frequency, or stocking volume. Thus, we call for empirical research on other variables that could explain a greater variety of reseller behaviour. It would be particularly interesting to examine if the simultaneous use of multiple marketing channels affected a reseller's behavioural sales intention and stocking behaviour.

Conclusion

The results of this study showed that two types of benefits determine the effectiveness of a cybersecurity supplier's digital channel marketing: relational and functional. The former refers to the perceived improvements in the quality of the relationship between suppliers and value-added resellers, and the latter refers to concrete tools and skills that the supplier can provide to the resellers. Conversely, the informativeness of communication, measured in terms of timely information about new offerings, upgrades, sales campaigns, and promotional offers does not increase the reseller's intention to sell the supplier's cybersecurity solutions. This finding is somewhat surprising, given that suppliers of IT products worldwide put a lot of effort into informing their resellers about price discounts and promotional campaigns. We believe that, because cybersecurity products are characteristically complex and difficult to comprehend by nature, price offers, campaigns, or even new product features are of little interest to value-added resellers. Rather, the resellers need to understand these solutions to be able to sell them at the first place. Cyber-threats are immense and beyond the control of the end customers, who are profoundly dependent on the knowledge of retailers who are selling cybersecurity solutions. In turn, these retailers become dependent on the supplier's technological and domain-specific expertise. Thus, we believe that cybersecurity solution providers, or providers of other complex technologies, who can assist their retailers to create clarity in technological complexity, will eventually gain respect and preferential status among the resellers.

Furthermore, the abundance of supplier's digital channel marketing does not seem to increase intention of value-added resellers to sell the supplier's cybersecurity products. It is likely that the ever-increasing complexity of cybersecurity solutions cause increased informational and cognitive demands for sales professionals, and the abundance of information per se – particularly related to provisional special pricing – does not alleviate their sales burdens. Again, value-added resellers are keen for practical sales tools that will improve their capability to understand and sell these solutions to end customers. Such tools may prove the most effective way of keeping the supplier's cybersecurity product and service brands at the forefront of the reseller's minds. In other words, we found that the marketing effectiveness of cybersecurity providers' digital channel marketing is contingent on the perceived quality rather than the quantity of digital channel marketing. These findings are important for cybersecurity providers, because the perceived quality of digital channel marketing has a direct influence on the intentions of value-added resellers to sell the supplier's cybersecurity products, which ultimately leads to stocking decisions. In addition, the findings support previous findings by, for example, Andersen (2001), who found that marketing communication is connected with relationship development, and a receiver's commitment to the sender is preceded by awareness and persuasion. The findings also support the work of Kauppila and colleagues (2010), who argue that social support from developers improves a salesperson's motivation and decreases their reluctance to sell new technology. Hence, our contribution to theory is that the extent to which digital channel marketing can strengthen the relationship between supplier and value-added reseller and improve the reseller's capabilities to sell cybersecurity solutions to end customers will ultimately determine the effectiveness of channel marketing.

The study offers some practical implications for cybersecurity solution providers, especially for those wishing to benefit from the growing market for cybersecurity products among small and midsized businesses. First, providers should leverage the power of resellers to better reach the fragmented market. However, they have to plan their marketing strategy appropriately. That is, instead of focusing on aggressive price discounts, promotional campaigns, and updates on new features and versions, cybersecurity providers should focus on helping their resellers to understand, communicate, and deliver the value of their cybersecurity solutions to the end customers in the first place. Also, they should pay attention to the quality of interaction with their value-added resellers, because it has the potential to strengthen or weaken supplier-reseller relationships. In particular, a supplier's digital channel marketing

Effective Digital Channel Marketing for Cybersecurity Solutions

Mika Westerlund and Risto Rajala

should focus on building reciprocal trust and commitment that would result in closer and deeper relationships. Second, cybersecurity suppliers should use digital channel marketing to provide their resellers with concrete sales tools and skills. Value-added resellers commit to sell a cybersecurity solution only if they are able to understand the solution and its value to end customers. The essence of digital channel marketing is to decrease technology and exchange uncertainty and to strengthen collaboration and commitment between suppliers and resellers for improved sales performance.

About the Authors

Mika Westerlund, D. Sc. (Econ.), is an Assistant Professor at Carleton University's Sprott School of Business in Ottawa, Canada. He previously held positions as a Postdoctoral Scholar in the Haas School of Business at the University of California Berkeley, in the United States, and in the School of Economics at Aalto University in Helsinki, Finland. Mika earned his first doctoral degree in Marketing from the Helsinki School of Economics in Finland. He is also a PhD student at Aalto University in the Department of Industrial Engineering and Management. His current research interests include user innovation, industrial ecology, business strategy, and management models in high-tech and service-intensive industries.

Risto Rajala, D.Sc. (Econ), is an Assistant Professor in the Department of Industrial Engineering and Management at Aalto University in Helsinki, Finland. Dr. Rajala holds a PhD in Information Systems Science from the Aalto University School of Business. His recent research concerns the management of complex service systems, development of digital services, service innovation, and business model performance. Rajala's specialties include management of industrial services, collaborative service innovation, knowledge management, and design of digital services.

References

Ajzen, I. 1985. From Intentions to Actions: A Theory of Planned Behavior. In J. Kuhl & J. Beckmann (Eds.), *Action Control: From Cognition to Behavior*. New York: Springer-Verlag.

Andersen, P. H. 2001. Relationship Development and Marketing Communication: An Integrative Model. *Journal of Business & Industrial Marketing,* 16(3):167-182. http://dx.doi.org/10.1108/08858620110389786

Barry, J., & Terry, T. S. 2008. Empirical Study of Relationship Value in Industrial Services. *Journal of Business & Industrial Marketing,* 23(4): 228–241. http://dx.doi.org/10.1108/08858620810865807

Bentler, P. M., & Chou, C.-P. 1987. Practical Issues in Structural Modeling. *Sociological Methods and Research,* 16(1): 78-117. http://dx.doi.org/10.1177/0049124187016001004

Chin, W. W., Marcolin, B. L., & Newsted, P. R. 2003. A Partial Least Squares Latent Variable Modeling Approach for Measuring Interaction Effects: Results from a Monte Carlo Simulation Study and an Electronic-Mail Emotion/Adoption Study. *Information Systems Research,* 14(2): 189-217. http://dx.doi.org/10.1287/isre.14.2.189.16018

Chung, C., Chatterjee, S. C., & Sengupta, S. 2012. Manufacturers' Reliance on Channel Intermediaries: Value Drivers in the Presence of a Direct Web Channel. *Industrial Marketing Management,* 41(1): 40–53. http://dx.doi.org/10.1016/j.indmarman.2011.11.010

Corsaro, D., & Snehota, I. 2010. Searching for Relationship Value in Business Markets: Are We Missing Something? *Industrial Marketing Management,* 39(6): 986–995. http://dx.doi.org/10.1016/j.indmarman.2010.06.018

Craigen, D., Diakun-Thibault, N., & Purse, R. 2014. Defining Cybersecurity. *Technology Innovation Management Review,* 4(10): 13–21. http://timreview.ca/article/835

Danaher, P. J., & Rossiter, J. R. 2011. Comparing Perceptions of Marketing Communication Channels. *European Journal of Marketing,* 45(1/2): 6-42. http://dx.doi.org/10.1108/03090561111095586

Diamantopoulos, A., & Siguaw, J. 2000. *Introducing Lisrel: A Guide for the Uninitiated.* London: SAGE.

Edwards, T., Battisti, G., & Neely, A. 2004. Value Creation and the UK Economy: A Review of Strategic Options. *International Journal of Management Reviews,* 5(3-4): 191–213. http://dx.doi.org/10.1111/j.1460-8545.2004.00103.x

Eggert, A., Ulaga, W., & Schultz, F. 2006. Value Creation in the Relationship Life Cycle: A Quasi-Longitudinal Analysis. *Industrial Marketing Management,* 35(1): 20-27. http://dx.doi.org/10.1016/j.indmarman.2005.07.003

Fishbein, M. & Ajzen, I. 1975. *Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research.* Reading, MA: Addison-Wesley.

Fornell, C., & Larcker, D. F. 1981. Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research,* 18(1): 39–50. http://www.jstor.org/stable/3151312

Effective Digital Channel Marketing for Cybersecurity Solutions

Mika Westerlund and Risto Rajala

Hansen, H., Samuelsen, B. M., & Silseth, P. R. 2008. Customer Perceived Value in B-to-B Service Relationships: Investigating the Importance of Corporate Reputation. *Industrial Marketing Management,* 37(2): 206-217. http://dx.doi.org/10.1016/j.indmarman.2006.09.001

Holden-Bache, A. 2011. Study: 93% of B2B Marketers Use Social Media Marketing. *Social Media B2B.* October 1, 2014: http://socialmediab2b.com/2011/04/93-of-b2b-marketers-use-social-media-marketing/

Hughes, D. E., & Ahearne, M. 2010. Energizing the Reseller's Sales Force: The Power of Brand Identification. *Journal of Marketing,* 74(4): 81-96. http://dx.doi.org/10.1509/jmkg.74.4.81

Hughes, D.E. 2013. This Ad's for You: The Indirect Effect of Advertising Perceptions on Salesperson Effort and Performance. *Journal of the Academy of Marketing Science,* 41(1): 1-18. http://dx.doi.org/10.1007/s11747-011-0293-y

Jerman, D., & Zavrsnik, B. 2012. Model of Marketing Communications Effectiveness in the Business-to-Business Markets. *Economic Research - Ekonomska Istrazivanja,* 25(1): 364-388.

Johanson, D. 2013. The Evolving U.S. Cybersecurity Doctrine. *Security Index: A Russian Journal on International Security,* 19(4): 37-50. http://dx.doi.org/10.1080/19934270.2013.846072

Kalyanam, K., & Brar, S. 2009. From Volume to Value: Managing the Value-Add Reseller Channel at Cisco Systems. *California Management Review,* 52(1): 94-119. http://www.jstor.org/stable/10.1525/cmr.2009.52.1.94

Kumar, N., Stern, L. W., & Achrol, R. S. 1992. Assessing Reseller Performance From the Perspective of the Supplier. *Journal of Marketing Research,* 29(2): 238-253. http://www.jstor.org/stable/3172573

Lemmink, J., de Ruyter, K., & Wetzels, M. 1998. The Role of Value in the Delivery Process of Hospitality Services. *Journal of Economic Psychology,* 19(2): 159-177. http://dx.doi.og/10.1016/S0167-4870(98)00002-6

Lilien, G. L., Grewal, R., Bowman, D., Ding, M., Griffin, A., Kumar, V., Narayandas, D., Peres, R., Srinivasan, R., & Wang, Q. 2010. Calculating, Creating, and Claiming Value in Business Markets: Status and Research Agenda. *Marketing Letters,* 21(3): 287-299. http://dx.doi.org/10.1007/s11002-010-9108-z

Lindgreen, A., & Wynstra, F. 2005. Value in Business Markets: What Do We Know? Where Are We Going? *Industrial Marketing Management,* 34(7): 732-748. http://dx.doi.org/10.1016/j.indmarman.2005.01.001

Lindgreen, A., Palmer, R., Vanhamme, J., & Wouters, J. 2006. A Relationship-Management Assessment Tool: Questioning, Identifying, and Prioritizing Critical Aspects of Customer Relationships. *Industrial Marketing Management,* 35(1): 57-71. http://dx.doi.org/10.1016/j.indmarman.2005.08.008

Menon, A., Homburg, C., & Beutin, N. 2005. Understanding Customer Value in Business-to-Business Relationships. *Journal of Business-to-Business Marketing,* 12(2): 1-38. http://dx.doi.org/10.1300/J033v12n02_01

Mohr, J., & Spekman, R. 1994. Characteristics of Partnership Success: Partnership Attributes, Communication Behavior, and Conflict Resolution Techniques. *Strategic Management Journal,* 15(2): 135-52. http://dx.doi.org/10.1002/smj.4250150205

Payne, A., & Holt, S. 2001. Diagnosing Customer Value: Integrating the Value Process and Relationship Marketing. *British Journal of Management,* 12(2): 159-182. http://dx.doi.org/10.1111/1467-8551.00192

Rahmani, Z., Mojaveri, H.S., & Allahbakhsh, A. 2012. Review the Impact of Advertising and Sale Promotion on Brand Equity. *Journal of Business Studies Quarterly,* 4(1): 64-73.

Rapp, A., Beitelspacher, L. S., Grewal, D., & Hughes, D. E. 2013. Understanding Social Media Effects Across Seller, Retailer, and Consumer Interactions. *Journal of the Academy of Marketing Science,* 41(5): 547-566. http://dx.doi.org/10.1007/s11747-013-0326-9

Ringle, C. M., Wende, S., & Will, S. 2005. SmartPLS 2.0 (M3) Beta, Hamburg. http://www.smartpls.de

Simpson, P. M., Siguaw, J. A., & Baker, T. L. 2001. A Model of Value Creation – Supplier Behaviors and Their Impact on Reseller-Perceived Value. *Industrial Marketing Management,* 30(2): 119-134. http://dx.doi.org/10.1016/S0019-8501(00)00138-3

Sreenivas, M., & Srinivas, T. 2008. Effectiveness of Distribution Network. *International Journal of Information Systems and Supply Chain Management,* 1(1): 80-86. http://dx.doi.org/10.4018/jisscm.2008010105

Tenenhaus, M., Vinzi, V. E., Chatelin, Y.-M., & Lauro, C. 2005. PLS path modeling. *Computational Statistics and Data Analysis,* 48(1): 159-205. http://dx.doi.org/10.1016/j.csda.2004.03.005

Teo, H. H., Kwok, K. W., & Benbasat, I. 2003. Predicting Intention to Adopt Interorganizational Linkages: An Institutional Perspective. *MIS Quarterly,* 27(1): 19-49. http://www.jstor.org/stable/30036518

The 2112 Group. 2014. *The Power of Multiples: Best Practices for Selling Best-of-Breed Solutions.* Port Washington, NY: The 2112 Group.

Ulaga, W. 2003. Capturing Value Creation in Business Relationships: A Customer Perspective. *Industrial Marketing Management,* 32(8): 677-693. http://dx.doi.org/10.1016/j.indmarman.2003.06.008

Walters, D., & Lancaster, G. 2000. Implementing Value Strategy through the Value Chain. *Management Decision,* 38(3):160-178. http://dx.doi.org/10.1108/EUM0000000005344

Webster, F. E., Jr. 2000. Understanding the Relationships among Brands, Consumers, and Resellers. *Journal of the Academy of Marketing Science,* 28(1): 17–23. http://dx.doi.org/10.1177/0092070300281002

Villarejo-Ramos, A. F. 2005. The Impact of Marketing Communication and Price Promotion on Brand Equity. *Journal of Brand Management,* 2(6): 431-444. http://dx.doi.org/10.1057/palgrave.bm.2540238

Wold, H. 1982. Systems under Indirect Observation Using PLS. In: C. Fornell (Ed.), *A Second Generation of Multivariate Analysis:* 325-347. Praeger, New York.

Effective Digital Channel Marketing for Cybersecurity Solutions

Mika Westerlund and Risto Rajala

Appendix 1. About the Research

We applied the partial least squares (PLS) method of analysis suggested by Wold (1982) to estimate the parameters. First, we ensured that our data of 109 companies and 15 indicators meets the guideline of five or more respondents per indicator (cf. Bentler and Chou, 1987). Second, we examined composite reliability values (ρc) and average variance extracted values (ρv) for each latent variable to assess the reliability and validity of the constructs. The scales seem to perform amply: ρc exceeded the recommended minimum level of .70 (cf. Fornell and Larcker, 1981) and ρv exceeded the .50 benchmark (cf. Diamantopoulos and Siguaw, 2000). Table 2 shows these values as well as means, standard deviations, and correlations for the constructs.

We examined the correlation matrix of the constructs in order to assess discriminant validity. Fornell and Larcker (1981) put forward that satisfactory discriminant validity among constructs is obtained when the square root of the average variance extracted is greater than corresponding construct correlations. In our data, the square root of the average variance extracted exceeded their correlations for each pair of first-order constructs (see numbers in parentheses in Table 1). All constructs met the criterion, which supports the discriminant validity of the constructs. The scale items used in the survey, as well as constructs and are listed in Table 3.

The PLS path modelling approach does not include proper single goodness of fit measure, but we used the global fit measure (GoF) suggested by Tenenhaus and colleagues (2005) to evaluate the goodness of fit in our model. Given that the criteria for small, medium, and large effect sizes are .10, .25, and .36, the GoF of our model (.46) indicates a good fit to the data. Furthermore, we assessed the explanatory power of the model for the dependent constructs by measuring their squared multiple correlations value (R^2). The independent variables were able to explain 62.3 percent of the variation in reseller's behavioural sales intention and 17.2 percent of the resulting stocking decision, both of which are considered appropriate.

Table 2. Construct correlations and descriptive statistics of measures

Construct	Mean	SD	ρ_v	ρ_c	1	2	3	4	5	6
1. Functional benefits	3.15	1.07	.86	.93	(.93)					
2. Informative benefits	3.69	0.83	.71	.88	.51	(.84)				
3. Stocking decision	1.94	0.91	.85	.92	.35	.12	(.92)			
4. Relational benefits	2.80	0.92	.84	.94	.60	.58	.23	(.92)		
5. Sales intention	2.64	0.98	.83	.91	.75	.42	.41	.63	(.91)	
6. Marketing abundance	2.39	0.76	.67	.86	.46	.59	.22	.72	.49	(.82)

Citation: Westerlund, M., & Rajala, R. 2014. Effective Digital Channel Marketing for Cybersecurity Solutions. *Technology Innovation Management Review*, 4(10): 22–32. http://timreview.ca/article/836

Keywords: cybersecurity, retailer, value-added reseller, VAR, supplier, marketing, sales, digital channel marketing

Effective Digital Channel Marketing for Cybersecurity Solutions

Mika Westerlund and Risto Rajala

Table 3. Scale items and constructs

Quality of Digital Channel Marketing			
Item	Loading	Weight	Item description
RELATIONAL BENEFITS			*Modified from Walters & Lancaster (2000); Andersen (2001); Corsaro & Snehota (2010); Eggert et al. (2006).*
K12	.89	.35	Supplier's digital channel marketing (DCM) improves collaboration in our supplier-reseller relationship.
K13	.93	.36	Supplier's DCM builds our reciprocal trust
K14	.94	.38	Supplier's DCM augments long-lasting and close relationship with us
INFORMATIVE BENEFITS			*Modified from Martin et al. (2003); Villarejo-Ramos (2005); Eggert et al. (2006).*
K7	.92	.53	Receiving ongoing sales campaigns and promotional offers is important
K8	.90	.38	Information about new offerings and upgrades are valuable for us
K9	.68	.26	Information about upcoming events and seminars are valuable for us
FUNCTIONAL BENEFITS			*Modified from Lindgreen et al. (2006).*
K17	.93	.56	Supplier's DCM improves our sales skills and capabilities
K18	.92	.52	Supplier's DCM provides us with practical sales tools
Quantity of Digital Channel Marketing			
Item	Loading	Weight	Item description
MARKETING ABUNDANCE			*Modified from Jerman & Zavrsnik (2012).*
K11	.89	.45	I prefer working with suppliers that are very active in digital channel marketing
K16	.80	.43	I highly value suppliers that send marketing messages frequently
K5	.78	.34	I receive marketing messages from the suppliers not too often
Sales Intention			
Item	Loading	Weight	Item description
K19	.92	.58	I put extra effort in selling products that suppliers provide with plenty of information
K21	.90	.52	I prefer selling products we have obtained digital marketing messages of
Stocking Decision			
Item	Loading	Weight	Item description
K20	.90	.51	I often buy to stock products actively marketed by the supplier
K22	.93	.58	I often buy to stock campaign products marketed by the supplier

Note: The response options ranged from 1 = "strongly disagree" to 5 = "strongly agree".

Cybersecurity Capability Maturity Models for Providers of Critical Infrastructure

Walter Miron and Kevin Muita

> *"The truth is rarely pure and never simple."*
>
> Oscar Wilde (1854–1900)
> Writer, poet, and playwright

Critical infrastructure such as power generation and distribution systems, telecommunications networks, pipelines and pipeline control networks, transportation control networks, financial networks, and government information and communications technology (ICT) have increasingly become the target of cyber-attacks. The impact and cost of these threats, as well as regulatory pressure to mitigate them, have created an impetus to secure these critical infrastructures. Managers have many controls and models at their disposal to help them secure infrastructure technology, including cybersecurity capability maturity models to enable measurement and communication of cybersecurity readiness to top management teams, regulators, and customers, thereby facilitating regulatory compliance, corporate responsibility, and improved brand quality. However, information and awareness is lacking about which models are most appropriate for a given situation and how they should be deployed.

This article examines relevant cybersecurity capability maturity models to identify the standards and controls available to providers of critical infrastructure in an effort to improve their level of security preparedness. These capability models are described and categorized by their relevance to different infrastructure domains, and then recommendations are provided on employing capability maturity models to measure and communicate readiness. This article will be relevant to regulators, critical infrastructure providers, and researchers.

Introduction

The critical infrastructures that make our way of life possible are increasingly vulnerable to cyber-attack. These critical infrastructures are defined as assets or systems required for the security and well being of citizens, including systems to produce and distribute water, electricity, and fuel, and communication networks (Public Safety Canada, 2009; Yusta et al., 2011; European Commission, 2013; U.S. Department of Homeland Security, 2013). Accordingly, disruption to one or more of these critical infrastructures usually incurs substantial human and financial cost, which is often the point of a cyber-attack and the reason such infrastructures are targeted by actors who may be motivated by profit or sociopolitical causes, among other motivations (Grau & Kennedy, 2014).

As the types of connectivity and volumes of data flow increase, the potential for cyber-attacks increases (Dupont, 2013) and brings greater focus on the security of critical infrastructures. In preparing their systems to withstand cyber-attacks, operators of critical infrastructure are faced with myriad controls and standards, and many of their implementations are incomplete or inconsistent, which further exacerbates the threat environment and provides a false sense of security (Chaplin & Akridge, 2005). To properly secure critical infrastructure and accurately report on its readiness to withstand cyber-threats, operators need a common measurement apparatus in addition to standard controls.

Providers of critical infrastructure have turned to cybersecurity capability maturity models to provide a framework for assessing and reporting cybersecurity

Cybersecurity Capability Maturity Models for Providers of Critical Infrastructure

Walter Miron and Kevin Muita

readiness. A capability maturity model improves the maturity and efficacy of controls employed to secure critical infrastructures. Such models delineate a sequence of maturity levels for a class of objects and represent an anticipated, desired, or typical evolution path of these objects shaped as discrete stages (Becker et al., 2009). This evolution should be sequential in nature and should have defined criteria for measurement (Wendler, 2012). A cybersecurity capability maturity model should be interpreted by subsector organizations of various types, structures, and sizes for the purpose of augmenting existing enterprise cybersecurity plans (U.S. Department of Energy, 2014). Cybersecurity capability maturity models have been developed for specific industry subsectors, but government implementation methods vary globally: public-private collaborations are the most common form of implementation in the United States and Canada, whereas regulatory schemas are more common in Europe and elsewhere (Yusta et al., 2011). And, as we will show in this article, the existing models tend to be descriptive, not prescriptive, in nature.

Given that cybersecurity is a global priority and a shared responsibility, there should be adequate motivation to develop more comprehensive critical infrastructure definitions and cybersecurity capability maturity models (Agresti, 2010). But, unfortunately, as we argue in this article, our toolkit of cybersecurity capability maturity models is itself insufficiently mature to address the full extent and magnitude of cyber-threats facing critical infrastructure today.

The purpose of this article is to examine current cybersecurity maturity models and evaluate their applicability to providers of interdependent critical infrastructures such as municipal governments. It contributes to practice by identifying a new category for assessing cybersecurity issues resulting from the interdependency of critical infrastructure. The article also highlights a gap in the existing cybersecurity literature relative to the adoption of capability maturity models by operators of interdependent critical infrastructures such as municipalities, which are often responsible for power, water, and emergency services, for example. By understanding this new category, researchers and practitioners alike will be better equipped to influence adoption of capability maturity models in securing and reporting on critical infrastructure cybersecurity readiness.

The article is organized as follows. First, we examine definitions of critical infrastructure and related regulatory frameworks in the European Union, the United States, and Canada. Next, we outline common threats to critical infrastructure. Then, we review and categorize the characteristics of current cybersecurity capability maturity models and their applicability to critical infrastructure operators, particularly those who have interdependent systems, such as municipalities. Finally, we offer managerial recommendations for employing cybersecurity capability models, identify gaps in the literature, and highlight areas for further study.

What is Critical Infrastructure?

Critical infrastructure includes any element of a system that is required to maintain societal function, maintain health and physical security, and ensure social and economic welfare (Yusta et al., 2011). Widely accepted examples of critical infrastructure are energy and utilities, financial systems, food, transportation, government, information and communications technology, health, and water purification and distribution. However, these elements do not operate in isolation today. Increasingly, connectivity and interdependencies between such systems increase the complexity of managing critical infrastructure and modelling the risks of cybersecurity threats (Rahman et al., 2011; Xioa-Juan & Li-Zhen, 2010). Indeed, Xiao-Juan and Li-Zhen (2010) state that "the computerization and automation of critical infrastructures have led to pervasive cyber interdependencies". And, Rahman, Martí, and Srivastava (2011) discuss the difficulty in assessing the effects that failures in communications networks may have on municipal infrastructures such as hospitals and emergency services. They further state that cyber-interdependencies comprise a fundamental class of interdependency in critical infrastructure networks.

To help cope with the security risks associated with the complexity and interdependencies within various critical infrastructure systems, standards bodies and federal agencies in at least twelve countries or regions have defined criteria for security standards as well as implementation methods (Yusta et al., 2011). For example, the European Union (EU) has moved towards a legislated critical infrastructure regimen through the European Programme for Critical Infrastructure Protection (EPCIP), and the United States has adopted a cooperative model between the Department of Homeland Security and industry with the National Infrastructure and Protection Plans of 2009 and 2013. In Canada and the United Kingdom, cooperative frameworks are also in place through the National Strategy for Critical Infrastructure and the Centre for the Protection of National

Cybersecurity Capability Maturity Models for Providers of Critical Infrastructure

Walter Miron and Kevin Muita

Infrastructure, respectively (Table 1). As a EU member, the United Kingdom has authored its own framework as recommended in the EPCIP.

In these four examples of federal government regulatory frameworks, only the EPCIP legislates a response from government and industry operators of critical infrastructure. In the EPCIP, obligations on EU nations are specified and supports are made available for EPCIP adoption by member states. In each of the remaining three examples – Canada, the United Kingdom, and the United States – a cooperative framework between government and operators is employed to foster communication of best practices for critical infrastructure and threats against it. These frameworks rely on adoption by operators rather than mandating compliance.

The literature on critical infrastructure emphasizes the importance and difficulty of assessing the cybersecurity readiness of interdependent networks. Each of the four frameworks in Table 1 recognizes interdependencies of critical infrastructure based on geographic considerations and specifies that collaboration is required to ensure an adequate response to critical infrastructure failures. However, when defined critical infrastructure such as water and power distribution, traffic control, emergency services, and the like are considered, the linkage between interdependent critical infrastructure and municipal governments as operators of multi-faceted critical infrastructure becomes apparent. Municipal governments require a framework suitable for evaluating and reporting the readiness of their interdependent critical infrastructures.

Threats to Critical Infrastructure

As the complexity and interdependencies of critical infrastructure increase, providers of critical infrastructure must cope with increasing vulnerability of their management systems to cyber-threats. As outlined in the *US National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (Office of the US President, 2003), three effects may constitute vulnerability on a system:

1. *Direct infrastructure effect*: Cascading disruption or arrest of the functions of critical infrastructures or key assets through direct attacks on a critical node, system, or function.

2. *Indirect infrastructure effect:* Cascading disruption and financial consequences for government, society, and economy through public and private sector reactions to an attack.

3. *Exploitation of infrastructure:* Exploitation of elements of a particular infrastructure to disrupt or destroy another target.

The increasing complexity of such system vulnerabilities, and the complexity of the threats themselves, necessitates cooperation between the industry and the government. These existing and emerging trends lead to a requirement for the consistent implementation of cybersecurity by industry stakeholders, key infrastructure providers, and government in order to protect critical infrastructure vital to financial, commercial, and social well being.

Table 1. Examples of cybersecurity regulations and frameworks

Region	Regulation	Model
European Union	European Programme for Critical Infrastructure Protection (EPCIP) tinyurl.com/nwgajk2	Regulation
Canada	National Strategy for Critical Infrastructure (NSCI) tinyurl.com/qcvryqv	Cooperative Framework
United Kingdom	Centre for the Protection of National Infrastructure (CPNI) tinyurl.com/kuplrq5	Cooperative Framework
United States	National Infrastructure and Protection Plan (NIPP 2013) tinyurl.com/n5ppvhs	Cooperative Framework

Cybersecurity Capability Maturity Models for Providers of Critical Infrastructure

Walter Miron and Kevin Muita

Cybersecurity Capability Maturity Models

Increased awareness of threats to constituents, and compliance frameworks at the federal government and industry levels, have created a need to assess and report on the readiness of the critical infrastructure provider using cybersecurity capability maturity models. With their roots in the software industry, capability maturity models originally represented a path of improvements recommended for organizations that want to increase their software process capability (Wendler, 2012). Typically, a capability maturity model has two components: i) a means of measuring and describing the development of an object in a sequential manner showing hierarchical progression, and ii) criteria for measuring the capabilities of the objects such as conditions, processes, or application targets. Together, these components provide a sequence of maturity levels for a class of objects. In other words, a capability maturity model represents an anticipated, desired, or typical evolution path of these objects shaped as discrete stages (Becker et al., 2009). They allow an organization to examine its capabilities sequentially in multiple dimensions and show hierarchical progression, thereby generating yardsticks representing defined maturity levels.

The concept of capability maturity models has been extended to the domain of cybersecurity and can be applied to the protection of critical infrastructure. In lieu of simple checklists, managers now have well-defined criteria against which to measure the maturity of their preparedness against cyber-threats (Debreceny, 2006; Lahrmann et al., 2011; Siponen, 2002), with models shifting from early examples such as the International Organization for Standardization's Systems Security Engineering Capability Maturity Model (SSE-CMM), Citigroup's Information Security Evaluation Model (CITI-ISEM) and Computer Emergency Response Team / CSO Online at Carnegie Mellon University (CERT/CSO) around the turn of the century to modern initiatives such as the current International Organization for Standardization (ISO/IEC) standards, the National Institute of Standards and Technology (NIST) Cybersecurity framework, the U.S. Department of Energy's Cybersecurity Capability Maturity Model (C2M2), and the U.S. Department of Homeland Security's NICE-CMM released in 2014. These modern cybersecurity capability maturity models provide the stages for an evolutionary path to developing policies and processes for the security and reporting of cybersecurity readiness of critical infrastructure.

The U.S. Department of Energy's C2M2, as well as the companion capability maturity models ES-C2M2 and ONG-C2M2, provides a maturity model and evaluation tool to facilitate cybersecurity readiness for operators of energy production and distribution networks. However, this tool is specific to the energy sector, which limits its applicability.

The U.S. Department of Homeland Security's NICE-CMM and the Software Engineering Institute at Carnegie Mellon University focus on workforce development, process maturity, and operational resilience practices to aid organizations in cybersecurity readiness. They do not offer specific cybersecurity best practices, however. Additional frameworks must be employed in conjunction with these models.

The ISO standards provide guidance covering the range of device certification (ISO/IEC 15408), information security management systems (ISO/IEC 27001), and software security engineering processes (ISO/IEC 21827 or SSE-CMM). Used together, these standards provide a complementary regimen for an organization's cybersecurity readiness; however, navigating the many standards is complicated and has time and cost implications.

The NIST cybersecurity framework provides a set of activities to aid organizations in developing individual readiness profiles. Although this framework is robust, it relies on operators to voluntarily develop individual profiles for their organizations.

The models described here – and summarized in Table 2 – provide guidance for organizations to prepare cybersecurity readiness plans, but aside from the ISO standards, they offer only high-level advice, and many apply only to specific industry verticals. The ISO standards, while offering more specific advice, are complicated to implement and do not specifically address our operators of interdependent critical infrastructure such as municipal governments. Thus, a model specific to this category of operator is required to adequately prepare for the possible cyber-attacks on municipal critical infrastructure.

Adoption of Cybersecurity Capability Maturity Models

Our review of the available cybersecurity capability maturity models shows that they are complicated to implement, have time and cost implications, and an

Cybersecurity Capability Maturity Models for Providers of Critical Infrastructure

Walter Miron and Kevin Muita

Table 2. Cybersecurity capability maturity models for critical infrastructure

Model	Publisher	Purpose
C2M2 (tinyurl.com/kvtuacm)	US Dept. of Energy	Assessment of cybersecurity capabilities for any organization comprised of a maturity model and evaluation tool
ES-C2M2 (tinyurl.com/pe62edg)	US Dept. of Energy	C2M2 tailored to energy subsector
ONG-C2M2 (tinyurl.com/mx3qzyk)	US Dept. of Energy	C2M2 tailored to the oil and natural gas subsector
NICE-CMM (tinyurl.com/m3224qv)	US Dept. of Homeland Security	Defines three areas: process and analytics, integrated governance, skilled practitioners and technology for workforce development
CERT-RMM (tinyurl.com/mp85m7y)	CERT/SEI	Defines organizational practices for operational resilience, security, and business continuity
ISO/IEC 15408 (tinyurl.com/mvw3dxl)	ISO	Criteria for computer security certification
ISO/IEC 27001 (tinyurl.com/kh2t2uo)	ISO	Information Security Management System (ISMS) specification
ISO/IEC 21827 SSE-CMM (tinyurl.com/obfeup3)	ISO	Evaluation of software security engineering processes
NIST Cybersecurity Framework (tinyurl.com/kugdfug)	NIST	Framework for improving federal critical infrastructure through a set of activities designed to develop individual profiles for operators

organization's processes may need to be refined during implementation. However, three of the regulatory frameworks in Table 1 rely on their voluntary adoption by operators of critical infrastructure, leading us to ponder how adoption of these models can be fostered effectively in an unlegislated environment.

Rogers (1983) explains that large organizations such as municipalities can be seen as laggards in his diffusion of innovation adopter categories. Diffusion of innovation theory also identifies five factors that impact adoption: relative advantage (i.e., the value that the innovation provides over the current method); compatibility (i.e., how easily the innovation incorporates into the current routine), simplicity (i.e., whether the innovation is difficult to use); trialability (i.e., how easy it is to try the innovation without commitment); and observability (i.e., how visible the innovation is in a community of the adopter's peers). Considering these five factors and the adopter categories, several categories of motivators and capabilities must be addressed to prompt adoption of cybersecurity capability maturity models by a given operator.

For example, increased observability of vulnerabilities by a critical-infrastructure operator peer group can inform executives on the will and direction of their association and may form the impetus for adoption by the industry. Similarly, enhancing the regulatory frameworks shown in Table 1 or brand damage resulting from exploitation can inform executives on their obligations to securing critical infrastructure and form the impetus for adoption. The availability of applicable capability maturity models for the operator and competent staff may address the factors of simplicity and trialability. We contend that applying diffusion of innovation theory to assess adoption methods will help build a cybersecurity capability maturity model for operators of interdependent critical infrastructure such as municipal governments.

Cybersecurity Capability Maturity Models for Providers of Critical Infrastructure

Walter Miron and Kevin Muita

Conclusion

Modern society has become increasingly dependent on the computers and systems that control our critical infrastructure and in doing so have created a scenario whereby a cyber-attack can have serious impacts on our way of life. In the case of municipal governments that operate a network of interdependent systems, the impacts of such a cyber-attack could be far reaching. The unique properties and criticality of these entities constitutes a new category of critical infrastructure provider that warrants study.

Our review of the current cybersecurity capability maturity models highlighted that, although many models exist, none are specifically crafted to address the scenario of an operator of multiple interdependent systems. Rather, they are focused on federal infrastructures or specific industry sub-sectors, and are all at a high level. The absence of a cybersecurity capability maturity model for municipal governments provides an opportunity for further research to industry experts and researchers of cybersecurity capability maturity models.

Although the regulatory frameworks shown in Table 1 provide clear definitions of critical infrastructure and the need to secure them, they lacked a focus on adoption of cybersecurity capability maturity models, relying on operators to define and adopt best practices. We postulate that Rogers' (1983) diffusion of innovation theory can be applied when building and facilitating industry adoption of a cybersecurity capability maturity model for municipal operators of critical infrastructure, and this topic may be worthy of further study.

This article contributes to the literature in two ways.

1. It identifies a new category for operators of *interdependent networks of critical infrastructure*, highlighting the need for a cybersecurity capability maturity model for operators such as municipal governments.

2. It highlights a gap in the literature relative to the adoption of cybersecurity capability maturity models, particularly at the municipal level, providing an opportunity for further research.

In summary, this article discussed critical infrastructure, cybersecurity capability maturity models, and factors affecting their adoption. We found that there is an opportunity to develop a cybersecurity capability maturity model that better addresses the unique properties of operators of interdependent critical infrastructures. Researchers may seize the opportunities for further study on cybersecurity capability maturity models and their adoption. Operators should consider Rogers' five-factors when reviewing their plans for augmenting their cybersecurity readiness.

About the Authors

Walter Miron is a Director of Technology Strategy at TELUS Communications, where he is responsible for the evolution of their packet and optical networks. He has over 20 years of experience in enterprise and service provider networking conducting technology selection and service development projects. Walter is a member of the research program committee of the SAVI project, the Heavy Reading Global Ethernet Executive Council, and the ATOPs SDN/nFV Working Group. He is also Chair of the Venus Cybersecurity Corporation and a board member of the Centre of Excellence for Next Generation Networking (CENGN) in Ottawa, Canada. Walter is currently a graduate student in the Technology Innovation Management (TIM) program at Carleton University in Ottawa, Canada.

Kevin Muita is a graduate student in the Technology Innovation Management program at Carleton University in Ottawa, Canada. He has a Bachelor's degree in Technology from Africa Nazarene University in Nairobi, Kenya. He has co-founded two technology startups: a network consultancy company and a systems installation and maintenance company. He has experience in logistics and supply chain management, having managed a Coca-Cola distribution network in Kenya, overseeing a successful 300% increase in sales volume, operations, and service delivery.

Cybersecurity Capability Maturity Models for Providers of Critical Infrastructure

Walter Miron and Kevin Muita

References

Agresti, W. 2010.The Four Forces Shaping Cybersecurity. *Computer,* 43(2): 101-104. http://dx.doi.org/10.1109/MC.2010.53

Becker, J., Knackstedt, R., & Pöppelbuß, J. 2009. Developing Maturity Models for IT Management. *Business & Information Systems Engineering,* 1(3): 213-222. http://dx.doi.org/10.1007/s12599-009-0044-5

Chaplin, D. A., & Akridge, S. 2005. How Can Security Be Measured? *Information Systems Control Journal,* 2.

Debreceny, R. S. 2006. Re-Engineering IT Internal Controls: Applying Capability Maturity Models to the Evaluation of IT Controls. *Proceedings of the 39th Annual Hawaii International Conference on System Sciences:* 196c. http://dx.doi.org/10.1109/HICSS.2006.407

Dupont, B. 2013. Cybersecurity Futures: How Can We Regulate Emergent Risks? *Technology Innovation Management Review,* 3(7): 6-11. http://timreview.ca/article/700

European Commission. 2013. Critical Infrastructure. European Commission, Home Affairs. July 20, 2014: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/index_en.htm

Grau, D., & Kennedy, C. 2014. TIM Lecture Series – The Business of Cybersecurity. *Technology Innovation Management Review,* 4(4): 53-57. http://timreview.ca/article/785

Lahrmann, G., Marx, F., Mettler, T., Winter, R., & Wortmann, F. 2011. Inductive Design of Maturity Models: Applying the Rasch Algorithm for Design Science Research. In H. Jain, A. P. Sinha, & P. Vitharana (Eds.), *Service-Oriented Perspectives in Design Science Research:* 176–191. Berlin: Springer. http//dx.doi.org/10.1007/978-3-642-20633-7_13

Office of the US President. 2003. *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.* Washington, DC: The White House. http://www.dhs.gov/national-strategy-physical-protection-critical-infrastructure-and-key-assets

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

Rogers, E. M. 1983. *Diffusion of Innovations.* New York: Free Press.

Siponen, M. 2002. Towards Maturity of Information Security Maturity Criteria: Six Lessons Learned from Software Maturity Criteria. *Information Management & Computer Security,* 10(5): 210–224. http://dx.doi.org/10.1108/09685220210446560

U.S. Department of Energy. 2014. *Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model (ONG-C2M2 v1.1).* Washington, DC: U.S. Department of Energy. http://energy.gov/oe/downloads/oil-and-natural-gas-subsector-cybersecurity-capability-maturity-model-february-2014

U.S. Department of Homeland Security. 2013. What Is Critical Infrastructure? Washington, DC: U.S. Department of Homeland Security. July 20, 2014: http://www.dhs.gov/what-critical-infrastructure

Wendler, R. 2012. The Maturity of Maturity Model Research: A Systematic Mapping Study. *Information and Software Technology,* 54(12): 1317-1339. http://dx.doi.org/10.1016/j.infsof.2012.07.007

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

Yusta, J. M., Correa, G. J., & Lacal-Arántegui, R. 2011. Methodologies and Applications for Critical Infrastructure Protection: State-of-the-Art. *Energy Policy,* 39(10): 6100–6119. http://dx.doi.org/10.1016/j.enpol.2011.07.010

Citation: 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

Keywords: cybersecurity, critical infrastructure, capability maturity models, municipalities, standards, compliance, protection, regulation, framework, adoption

Q&A

Chen Han and Rituja Dongre

Q. What motivates cyber-attackers?

A. The need to understand the motivations of cyber-attackers is great, given that "cybersecurity risks pose some of the most serious economic and national security challenges of the 21st Century" (The White House, 2009). However, the motivations behind cyber-attacks intended to cause economic impacts may be different from those posing a threat to national security. And, in many cases, the real purpose and primary objective of a cyber-attack may be hidden or obscured, even if the attacker claims responsibility (Shakarian et al., 2013).

Nonetheless, to help tease out and understand common motivations, cyber-attackers may be categorized, noting that a given attacker may belong to more than one category (Andress & Winterfeld, 2011). For example, politically motivated cyber-attacks may be carried out by members of extremist groups who use cyberspace to spread propaganda, attack websites, and steal money to fund their activities or to plan and coordinate physical-world crime (Gandhi et al., 2011). Generally, the reason for non-politically motivated attacks is generally financial, and most attacks are considered as cyber-crime (Andreasson, 2011), but many cyber-attacks are motivated by deeply-rooted socio-cultural issues (Gandhi et al., 2011).

As shown in Figure 1, cyber-attackers can be broadly considered "insiders" or "outsiders" (Russell & Gangemi, 1993), meaning that they act from within an organization or attempt to penetrate it from the outside.

The three basic categories of insiders are: i) disgruntled employees, who may launch retaliatory attacks or threaten the safety of internal systems; ii) financially motivated insiders, who may misuse company assets or manipulate the system for personal gain (although some insiders may be acting on ethical grounds or for other reasons); and unintentional insiders, who may unwittingly facilitate outside attacks, but are not strictly speaking primary attackers (Andress & Winterfeld, 2011).

Outsiders can be classified based on their organization, motives, and professional level: organized attackers, hackers, and amateurs.

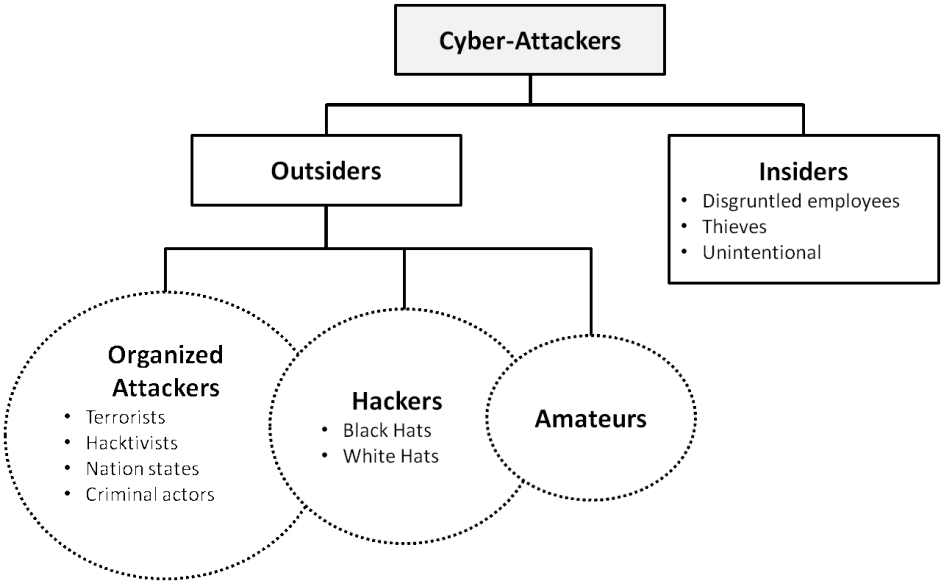

Figure 1. Categories of cyber-attackers

Q&A. What Motivates Cyber-Attackers?

Chen Han and Rituja Dongre

1. *Organized attackers:* include organizations of terrorists, hacktivists, nation states, and criminal actors. Terrorists are those who seek to make a political statement or attempt to inflict psychological and physical damage on their targets, in order to achieve their political gain or create fear in opponents or the public (Howard, 1997; Lewis, 2002; Cohen et al., 1998). Hacktivists seek to make a political statement, and damage may be involved, but the motivation is primarily to raise awareness, not encourage change through fear. Nation-state attackers gather information and commit sabotage on behalf of governments (Cohen et al., 1998), and are generally highly trained, highly funded, tightly organized, and are often backed by substantial scientific capabilities. In many cases, their highly sophisticated attacks are directed toward specific goals, but their specific motives may be mixed (Cohen et al., 1998). Criminal actors are usually "organized groups of professional criminals" (Cohen, et. al, 1998), and they may act within complex criminal ecosystems in cyberspace that are both "stratified and service oriented" (Grau & Kennedy, 2014). Perpetrators of organized crime are typically focused on control, power, and wealth (Gragido et al, 2012).

2. *Hackers:* may be perceived as benign explorers, malicious intruders, or computer trespassers (Hafner & Markoff, 1991; Lachow, 2009). This group includes individuals who break into computers primarily for the challenge and peer status attained from obtaining access (Howard, 1997). In some cases, hacking is not a malicious activity; a "white hat" hacker is someone who uncovers weaknesses in computer systems or networks in order to improve them, often with permission or as part of a contract with the owners. In contrast, "black hat" hacking refers to malicious exploitation of a target system for conducting illegal activities. In most cases, black hat hackers could be hired by or be sponsored by criminal organization or governments for financial gain or political purpose. Thus, hacking can involve espionage (i.e., to obtain secrets without the permission of the holder of the information, primarily for personal, political, or criminal purposes), extortion (i.e., to extract money, property, or other concessions by threatening harm), theft (i.e., to steal valuable data, information, intellectual property, etc.), vandalism (i.e., to cause damage) (Shakarian et. al, 2013; Cohen et. al, 1998; Howard, 1997).

3. *Amateurs:* less-skilled hackers, also known as "script kiddies" or "noobs" often use existing tools and instructions that can be found on the Internet. Their motivations vary: some may simply be curious or enjoy the challenge, others may be seeking to build up and demonstrate their skills to fulfill the entry criteria of a hacker group (Andress & Winterfeld, 2011). However benign their intentions may be, the tools used by amateurs can be very basic but powerful. Despite their lower skill skills, they can cause a lot of damage or, after gaining enough experience, may eventually "graduate" to professional hacking.

Although these categories are presented as discrete groups, there can be some overlap or difficulty placing a given situation into a particular box. For example, a group of hackers can act in a coordinated fashion, and in this sense could be considered "organized attackers."

The categories of cyber-attackers enable us to better understand the attackers' motivations and the actions they take. As shown in Figure 2, operational cybersecurity risks arise from three types of actions: i) inadvertent actions (generally by insiders) that are taken without malicious or harmful intent; ii) deliberate actions (by insiders or outsiders) that are taken intentionally and are meant to do harm; and iii) inaction (generally by insiders), such as a failure to act in a given situation, either because of a lack of appropriate skills, knowledge, guidance, or availability of the correct person to take action (Cebula & Young, 2010). Of primary concern here are deliberate actions, of which there are three categories of motivation (Gandhi et al., 2011):

1. *Political motivations:* examples include destroying, disrupting, or taking control of targets; espionage; and making political statements, protests, or retaliatory actions.

2. *Economic motivations:* examples include theft of intellectual property or other economically valuable assets (e.g., funds, credit card information); fraud; industrial espionage and sabotage; and blackmail.

3. *Socio-cultural motivations:* examples include attacks with philosophical, theological, political, and even humanitarian goals (Gradido et al., 2012). Socio-cultural motivations also include fun, curiosity, and a desire for publicity or ego gratification.

Q&A. What Motivates Cyber-Attackers?

Chen Han and Rituja Dongre

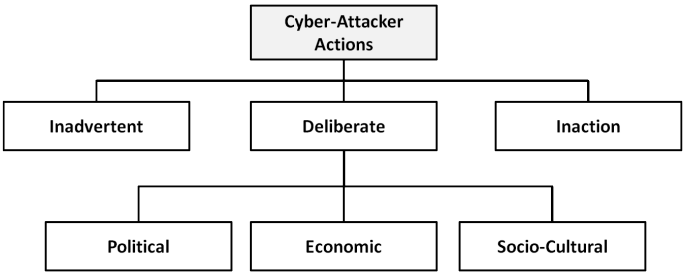

Figure 2. Types of cyber-attacker actions and their motivations when deliberate

About the Authors

Chen Han is a graduate student in the Technology Innovation Management (TIM) program at Carleton University in Ottawa, Canada. She has more than 8 years working experience in product design, User interface design and project management. She built and led an independent technical team that provides overall solutions and outsourcing services for various clients including world's top media, Internet startups, and multinational firms. Currently, she is working with founder team of Pricebeater, a global startup offering tools for online shopping in North America.

Rituja Dongre is a graduate student in Technology Innovation Management (TIM) program at Carleton University in Ottawa, Canada. She holds a Bachelor's Degree in Electronic and Telecommunication from the Nagpur University, India, and has worked as an Associate Consultant in Capgemini India.

Citation: Han, C., & Dongre, R. 2014. Q&A. What Motivates Cyber-Attackers? *Technology Innovation Management Review*, 4(10): 40–42.
http://timreview.ca/article/838

Keywords: motivation, cyber-attack, cybercrime, cybersecurity, hackers

References

Andreasson, K. J., 2011. Introduction. In K. J. Andreasson (Ed.), *Cybersecurity: Public Sector Threats and Responses:* XIII-XXV. Boca Raton, FL: CRC Press.

Andress, J., & Winterfeld, S., 2011. *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. Waltham, MA: Elsevier.

Cebula, J. J., & Young, L. R. 2010. *A Taxonomy of Operational Cyber Security Risks. Technical Note CEM/SEI-2010-TN-028.* Pittsburgh, PA: Software Engineering Institute.

Cohen, F., Phillips, C., Painton Swiler, L., Gaylor, T., Leary, P., Rupley, F., & Isler, R. 1998. A Cause and Effect Model of Attacks on Information Systems: Some Analysis Based on That Model, and The Application of That Model for Cyber Warfare in CID. *Computers & Security,* 17(3): 211-221.
http://dx.doi.org/10.1016/S0167-4048(98)80312-X

Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., & Laplante, P. 2011. Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political. *IEEE Technology and Society Magazine,* 30(1): 28-38.
http://dx.doi.org/10.1109/MTS.2011.940293

Gragido, W., Molina, D., Pierce, J., & Selby, N. 2012. *Blackhatonomics: An Inside Look at the Economics of Cybercrime*. Waltham, MA: Elsevier.

Grau, D., & Kennedy, C. 2014. TIM Lecture Series – The Business Of Cybersecurity. *Technology Innovation Management Review,* 4(4): 53–57.
http://timreview.ca/article/785

Hafner, K., & Markoff, J. 1991. *Cyberpunk: Outlaws and Hackers on the Computer Frontier*. New York: Simon & Schuster.

Howard, J. D. 1997. *An Analysis of Security Incidents on the Internet 1989–1995.* Doctoral Thesis, Carnegie-Mellon University, Pittsburgh, PA.

Lachow, I. 2009. Cyber Terrorism: Menace or Myth? In F. D. Kramer, S. H., Starr, & L. K. Wentz (Eds.), *Cyberpower and National Security:* 434-467. Dulles, VA: Potomac Books.

Lewis, J. A. 2002. *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats.* Washington, DC: Center for Strategic and International Studies.

Russell, D., & Gangemi, G. T. 1993. *Computer Security Basics.* Sebastopol, CA: O'Reilly & Associates.

Shakarian, P., Shakarian, J., & Ruef, A., 2013. *Introduction to Cyber-Warfare: A Multidisciplinary Approach*. Waltham, MA: Elsevier.

2009. *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure.* Washington, DC: Executive Office of the President of the United States.
http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

TIM Lecture Series
Cybersecurity Metrics and Simulation

George Cybenko

> *"Given the continual onslaught of successful cyber-attacks against banks, governments, and retailers, one has to wonder whether any progress is being made in computer security at all. How is it possible to reconcile the huge investments that have been made in securing networks and computers with the fact that attackers are still routinely breaching what should be highly protected networks? What metrics can explain the situation and how can we evaluate those metrics through simulation or other means?"*
>
> George Cybenko
> Professor of Engineering, Dartmouth College

Overview

The TIM Lecture Series is hosted by the Technology Innovation Management program (timprogram.ca) 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 sixth TIM lecture of 2014 was held at Carleton University on October 8th, and was presented by George Cybenko, the Dorothy and Walter Gramm Professor of Engineering at Dartmouth College in New Hampshire, United States. In the first part of his lecture, Cybenko provided an overview possible security metrics together with their pros and cons in the context of current IT security practices. In the second part of the lecture, Cybenko presented a modelling and simulation approach that produces meaningful quantitative security metrics as the basis for a more rigorous science of cybersecurity.

Summary

To begin his lecture, Cybenko highlighted the many high-profile cyber-attacks that dominate headlines today, which stand in contrast to massive investments in cybersecurity research and practices, as well as the creation of many cybersecurity companies, over the past 10 to 15 years. Thus, he then challenged the research community – himself included – to demonstrate greater progress over the next 10 years in terms of our capacity to mitigate the impacts of cyber-attacks. And, in introducing the key subject of his lecture, he pointed to the potential for cybersecurity metrics and simulation as a promising avenue to facilitate such progress.

To be effective, cybersecurity metrics should be:

1. *Reproducible:* when measuring a particular phenomenon, two people should be able to independently arrive at the same results.

2. *Relevant:* organizations must find the metrics operationally relevant and actionable.

3. *A basis for comparison:* metrics must facilitate comparisons between architectures, applications, systems, networks, etc.

4. *A basis for claims:* metrics must facilitate evaluations of systems and architectures to quantify their suitability to particular applications.

In developing metrics, we must also take into account the computer security lifecycle, which progresses from security concepts (i.e., an understanding of the technology and relevant threats), to architecture (i.e., an abstraction of the design), to implementation (i.e., code, hardware, support, and access), and then to operations (i.e., forensics on past events, real-time monitoring and patching of present conditions, and predicting future events). Metrics must be considered at each step in the lifecycle so that they can be effective once the operations stage is reached.

TIM Lecture Series – Cybersecurity Metrics and Simulation

George Cybenko

Next, Cybenko recognized a common skeptical view of security metrics, which, in its extreme form, rejects the need for metrics altogether, arguing that a system is either secure or it is not. However, when challenged to provide an example of a secure system, such skeptics struggle to come up with definitive examples. Thus, in practice, it is worthwhile recognizing a spectrum of computer security and using metrics to try to evaluate just how secure a given system is.

Proposed approaches to cybersecurity metrics include:

1. *Penetration testing:* automated tools that run a set of exploits against a network; by definition, penetration tests use only known exploits and cannot assess vulnerabilities or weaknesses that might be revealed by a human attacker.

2. *Red teams:* expert hackers hired to assess or attempt to break into a system; however, the perceived protection level is limited to the expenditure on testing (i.e., a company may pay a "Red Team" $X to assess a system, but hackers would expend effort exceeding $X to reach assets of greater value, and much greater human effort may expended for the same cost in countries where the labour rate is much lower).

3. *Compliance:* controls and standards for development, software, architecture, etc.; the protection level is only as good as the compliance standards; can redirect an organization's security expenditure away from novel and up-to-date approaches.

4. *Response times:* how quickly is a system patched? How quickly does an organization identify and respond to incidents? What is the optimal policy for disclosing vulnerabilities?

5. *Software size, complexity, and constructs:* may be indicators of security vulnerability

Each of these approaches has its benefits and shortcomings; however, it may be more useful to think about the field of cybersecurity metrics within the context of risk analysis. Thus, the expected cost of security may be calculated based on the probability and costs of potential losses. For example, in cases where expected losses due to fraud and intrusions exceed the costs of technology updates, the justification for improved technology becomes clear.

Next, in the second part of the lecture, Cybenko presented an alternative, simulation-based approach to cybersecurity metrics, which attempt to quantify cybersecurity. In particular, he focused on the QuERIES methodology, which was also detailed in Cybenko's 2013 article in the TIM Review (Hughes & Cybenko, 2013). The QuERIES methodology quantifies cybersecurity risk following an analogy from physical security, where the "time to compromise" in a system is a measureable performance metric. In cybersecurity, the time it takes an attacker to complete a successful attack against a protected software system provides a similar metric, which can be simulated and then presented in a probability distribution.

The QuERIES methodology simulates the value of success to an attacker if they are able to succeed within a particular amount of time. Thus, the value of the asset to an attacker changes over time because there is a cost to continued effort, and at some point, no amount of effort may be worth the value of the target asset. And, this type of risk-analysis approach is used to assess the progression of cyber-attack, it becomes possible to calculate the optimal time for an attacker to abandon an attack based on the cost of the attack and the value of the asset. Ideally, cybersecurity defenses could be sufficiently robust that the attacker's cost of attacking would be prohibitively high, and an attack would not even be initiated.

For a fuller explanation of the QuERIES methodology, see:

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

TIM Lecture Series – Cybersecurity Metrics and Simulation

George Cybenko

About the Speaker

George Cybenko is the Dorothy and Walter Gramm Professor of Engineering at Dartmouth College in New Hampshire, United States. He has made multiple research contributions in signal processing, neural computing, information security, and computational behavioural analysis. He was the Founding Editor-in-Chief of both IEEE/AIP Computing in Science and Engineering and IEEE Security & Privacy. He has served on the Defense Science Board (2008–2009), on the US Air Force Scientific Advisory Board (2012–2015), and on review and advisory panels for DARPA, IDA, and Lawrence Livermore National Laboratory. Cybenko is a Fellow of the IEEE and received his BS (Toronto) and PhD (Princeton) degrees in Mathematics.

This report was written by Chris McPhee.

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

Keywords: cybersecurity, metrics, simulation, modelling

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