Examining the Relationship between Cybersecurity and Scaling Value for New Companies

Tony Bailetti and Daniel Craigen

> *“All models are wrong, but some are useful.”*
>
> George Edward Pelham Box (1919 —2013),
> British statistician
> One of the great statistical minds of the 20th century

We explore the cybersecurity-scaling relationship in the context of scaling new company value rapidly. The relationship between the management of what a new company does to protect against the malicious or unauthorized use of electronic data, and the management of what a new company does to scale company value rapidly is important, but not well understood. We use a topic modelling technique to identify the eight topics that best describe a corpus comprised of 137 assertions about what new companies do to scale company value rapidly, manually examine the stability of the topics extracted from the dataset, and describe the relationship between 17 assertions about how to manage cybersecurity in new companies, and the six topics found to be stable. The six stable topics are labelled Fundraise, Enable, Position, Communicate, Innovate, and Complement. We find that of the 17 cybersecurity assertions, seven are related to Position, two to Innovate, one to Fundraise and, one to Complement. Six cybersecurity assertions were not found to be strongly related to any of the eight topics. This paper contributes to our understanding of cybersecurity in the context of a new company that scales its value rapidly, an application of topic modelling to perform small-scale data analysis, and a manual approach to examine the stability of the topics extracted by the topic modelling technique. We expect this paper to be relevant to new companies’ top management teams, members of the networks upon which new companies depend for to scale company value, accelerators and incubators, as well as academics teaching or carrying out research in entrepreneurship.

Introduction

The professional literature that examines the relationship between cybersecurity and company value is scant and underdeveloped. Moreover, we were not able to find a single article published in an academic journal that examined the relationship between cybersecurity and the growth of new companies in initial stages of development.

Increasingly, the professional literature is framing cybersecurity as a business enabler or an influencer rather than an overhead cost or an innovation blocker (Bello, 2019; Blivet, 2019; Cohen, 2019; Sloman, 2018; Trott, 2019; Watson, 2019). This literature urges companies’ security teams to deploy combinations of external and internal resources to create value and demonstrate that value (Trott, 2019).

The purpose of this paper is to increase our understanding of the relationship between cybersecurity (as represented by 17 assertions) and new companies that scale company value rapidly (as represented by 137 assertions, including the cybersecurity assertions).

The next sections of the paper provide a review of the literature in cybersecurity, describe the method used to explore the cybersecurity-scaling relationship, present and discuss the results, and summarize the conclusions.

Literature review

The professional literature describes the relationship between cybersecurity and growth of large businesses in several ways. These include factors such as how cyber security is represented at the board level (Trott, 2019; Watson, 2019), metrics used to demonstrate the value of cybersecurity to the business (CompTIA, 2019; Trott, 2019), customer loyalty (Cohen, 2019; Stoman, 2018), budget allocated to cybersecurity (Trott, 2019), extent to which security teams are overworked (Trott, 2019), preventative controls (Bello, 2019; Cohen, 2019), ability to anticipate sensitive activities (Trott, 2019), new territory expansion (Cohen, 2019), quality of responses to security breaches (Cohen, 2019), ability to trade-off cybersecurity and technology innovation (CompTIA, 2019), mobile employee empowerment (Bello, 2019), willingness to use third-party service providers (Blivett, 2019; Trott, 2019), quality of threat intelligence (Trott, 2019), increase trust in digital transformation (Trott, 2019), the workforce's level of expertise in cybersecurity (CompTIA, 2019), the level of security staff's skill in cybersecurity (CompTIA, 2019), and cybersecurity culture (Blivet, 2019).

The notion of "cybersecurity" has changed over time from data security, to computer security, and then to information security (Von Solms, 2013). This evolution has resulted in a strong technical engineering and computer science perspective for cybersecurity (Craigen et al., 2014; Ramirez, 2017; Soomro et al., 2016), along with an evolving perspective of what needs to be secured. At this point we believe that an understanding cybersecurity within a multidimensional (multidisciplinary) framework is now required.

In a 2018 commentary, Dennis Giever (Giever, 2018) argues that "we no longer have the luxury of allowing barriers to exist between those tasked with information technology security and those who provide physical security" and goes on to observe, more generally, that "Security has evolved into a rather complex enterprise which encompasses a wide range of fields". The literature review performed by (Soomro et al., 2016) reinforces the multidisciplinary perspective in arguing that information security needs a more holistic approach. They conclude by noting that "numerous activities of management, particularly development and execution of information security policy, awareness, compliance training, development of effective enterprise information architecture, IT infrastructure management, business and IT alignment and human resources management, had a significant impact on the quality of management of information security". Similarly, Kayworth and Whitten (2010) take the view that "information security strategy encompasses not only IT products and solutions but also organizational integration and social alignment mechanisms."

Questions have arisen as to whether cybersecurity is an enabler or a barrier to innovation. Nelson and Manick (2017) introduced a framework for evaluating the trade-offs. Based on their own literature review, they note that 10-15% of companies were above average in both innovation and cybersecurity maturity. These companies were called "secure digital innovators". Other companies were categorized as being reckless innovators (high innovation but low cybersecurity), secure conservatives (low innovation but high cybersecurity), or beginners (which were low in both). They also identified a number of factors that impact innovation and cybersecurity: the operating model and organizational structure; company culture and tensions created by cybersecurity efforts; boards of directors and their role in cybersecurity and innovation trade-off decisions; education, communication, and organizational awareness; legacy architectures; IT governance; and resource allocation.

Educational institutions are recognizing the need to complement technical competencies with nontechnical competencies. For example (Emmerson et al., 2019), the United States Naval Academy was amongst the first to develop an interdisciplinary pedagogical model that "blends technical courses such as programming and networks with nontechnical courses such as law, policy and ethics". In their program, they draw upon computer science, engineering, mathematics, psychology, law, political science, economics, and other fields, thereby providing "a holistic view of the threats, challenges and capabilities". This is something that would be missing if the focus is solely on technical knowledge.

The number of academic papers pertaining to cybersecurity has increased at a compound annual rate of 20% from 2004 to 2014 (Singer and Friedman, 2014). Yet, almost no one would claim that top management teams of new companies are more informed about the relationship between cybersecurity and scaling new company value.

Method

The objective is to better understand the relationship between the management of what a new company does to protect against the malicious or unauthorized use of electronic data, and the management of what a new company does to scale company value rapidly. We use 17 core assertions about cybersecurity (shown in Appendix A) to represent what a new company does to protect against the malicious or unauthorized use of electronic data. At the same time, we explore 137 assertions included in an inventory maintained by the SERS community (https://globalgers.org/) to represent what a new company does to scale company value rapidly.

The remainder of this section describes the four steps of the method used.

1. Developed topic model

A topic model is the best current approximation of finding K topics for a dataset with M documents and V unique words (Boyd-Graber et al., 2017).

Building on Boyd-Graber, Hu, and Mimno (2017), for this specific research study, by topic modelling we mean finding K topics for the following matrix formulation:

[M assertions x K topics] x [K topics x V unique words] ~ [M assertions x V unique words], where M equals 137 assertions and V equals 2,591, the latter which is the number of unique words used to express these assertions after 845 stopwords were excluded.

The first half of a topic model links K topics to "word piles". Thus, each topic represents a set of unique words extracted from the 137 assertions. Each topic gives higher weights to some words than others. The second half of the topic model links the K topics to individual assertions. Each assertion is about a small handful of topics, while most assertions have very low weights for most of the possible topics.

The topic-word relationship is based on how well a word fits with the topic. Words that fit a topic well will have higher weights than words that do not. The topic-assertion relationship is based on how well the topic expresses the assertion. Assertions that are expressed well by a topic will have higher weights for that topic.

We used Orange 3.24.1 (Orange, 2020) and the Latent Dirichlet Allocation (LDA) algorithm (Blei et al., 2003; Blei, 2012) to identify the latent topics that best describe the collection of 137 assertions about what a company does to scale company value rapidly.

The number of topics used to produce a topic model ranged from three to ten.

The decision on the number of topics for the final topic model was made by the authors of this paper based on a joint assessment of assertion weights per topic.

2.Determined topic stability

Four runs of the final topic model were performed. Topic stability was determined by assessing the consistency in which keywords appeared in the four runs of the final model, with topic quality assessed by the paper's authors (Xing & Paul, 2018). A topic was determined to be stable if five or more keywords appeared repeatedly in the four runs of the final model, and if the weights of the keywords on the topic were greater than 2. Topic quality was determined by the two authors.

3.Determined relationship between cybersecurity assertions and topics

A cybersecurity assertion was related to a topic if for each of the four runs the assertion loading in the topic was greater than 0.4.

4. Labelled and described topics

To label and succinctly describe each topic, we used keywords that appeared consistently in the four runs, the assertions that were related with the topic, and our background expertise.

Results

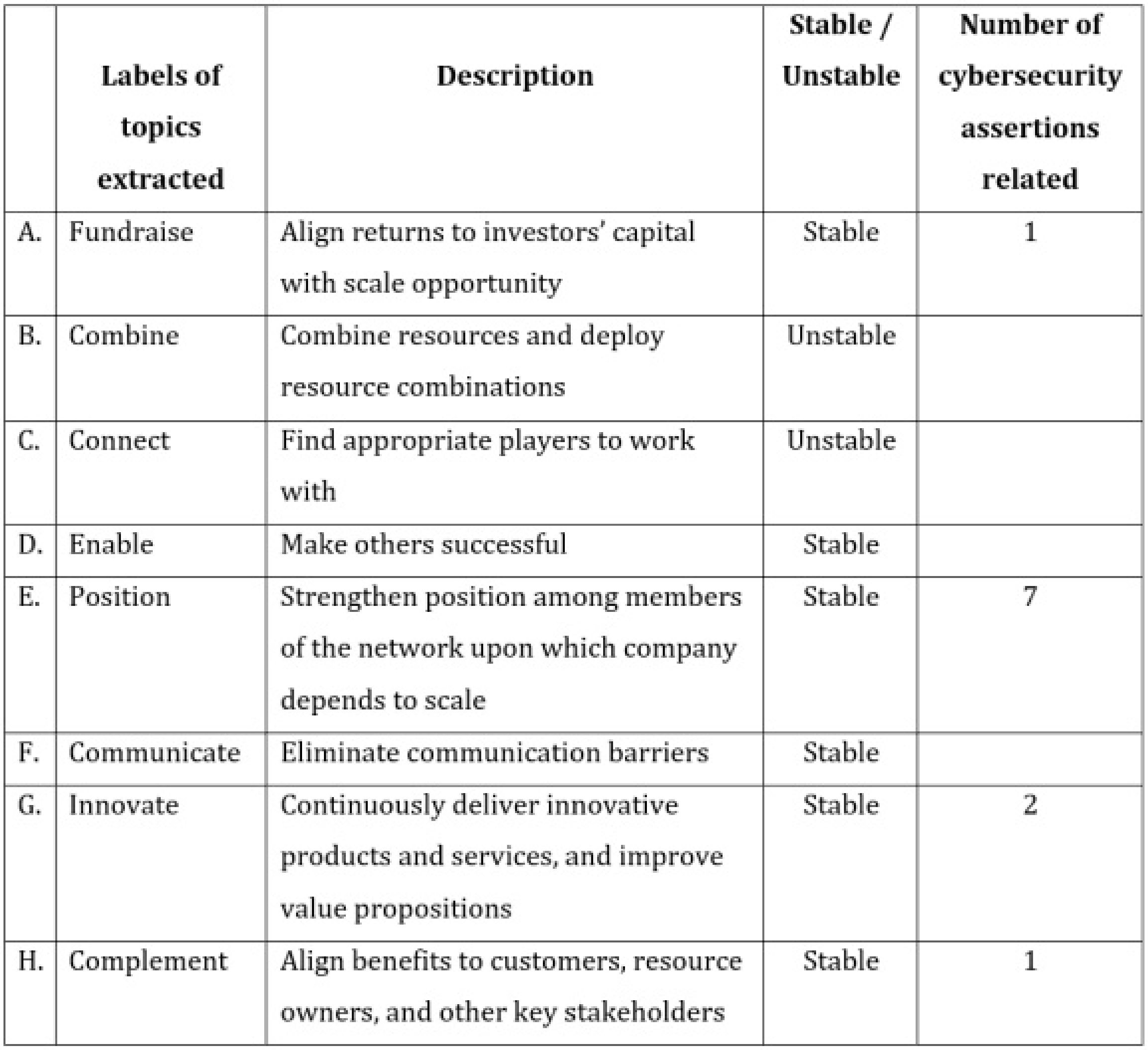
Corpus

The corpus is comprised of 137 assertions that are expressed using 2,591 words. On average, each assertion has 19 words. The assertions are included in the inventory of assertions maintained by the Scale Early, Rapidly and Securely (SERS) community. The SERS community is comprised of researchers and practitioners worldwide, who are committed to produce, disseminate, and evolve high quality resources about scaling companies (https://globalgers.org/). Each assertion is a clear and concise statement that describes an abstract company action, which can be detailed and then implemented to produce outcomes aimed at significantly and rapidly increasing the value of the new company. Each statement is transparent, traceable, and regionally inclusive.

Topic model

The authors decided that the best topic model generated by the research was the one that had eight topics. This decision was made for two reasons. First, the number of assertions that had topic loadings greater than .6 was at least three for each of the four runs of the eight-topics model. The second reason was that the topics of the eight-topic model made the most sense to the two authors given their understanding of the SERS assertions

Table 1. Topics extracted and number of cybersecurity assertions related to them



	Labels of topics extracted	Description	Stable / Unstable	Number of cybersecurity assertions related
A.	Fundraise	Align returns to investors' capital with scale opportunity	Stable	1
B.	Combine	Combine resources and deploy resource combinations	Unstable	
C.	Connect	Find appropriate players to work with	Unstable	
D.	Enable	Make others successful	Stable	
E.	Position	Strengthen position among members of the network upon which company depends to scale	Stable	7
F.	Communicate	Eliminate communication barriers	Stable	
G.	Innovate	Continuously deliver innovative products and services, and improve value propositions	Stable	2
H.	Complement	Align benefits to customers, resource owners, and other key stakeholders	Stable	1

inventory, and the subject of scaling company value rapidly.

Stable topics

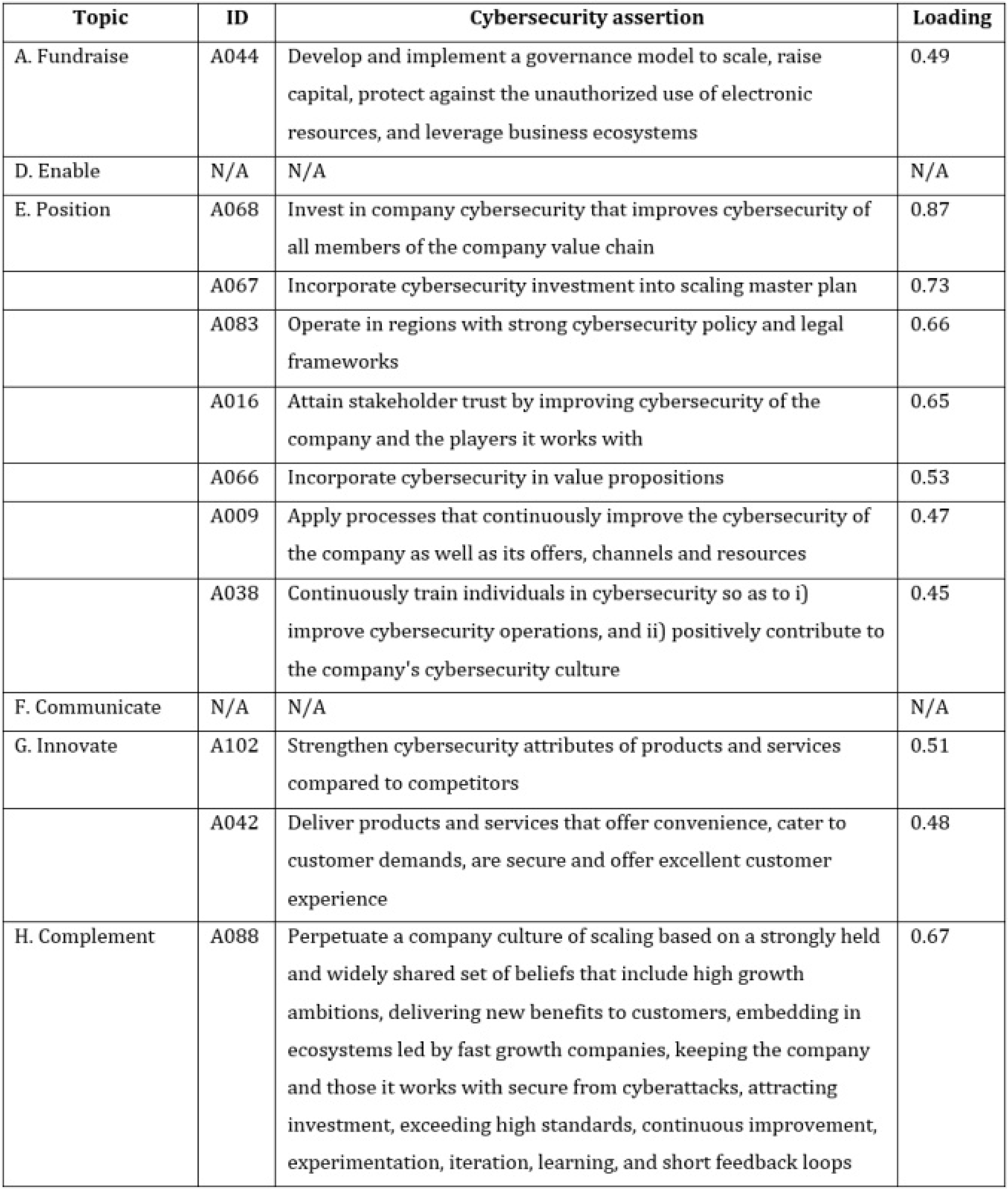
Table 1 provides the labels and succinct descriptions of the eight topics extracted from the collection of 137 assertions. For each topic, Table 1 shows whether the topic was stable or unstable, as well as the number of cybersecurity assertions that were related to it.

Our results suggest that six topics were stable: Fundraise, Enable, Position, Communicate, Innovate, and Complement. Two topics were deemed unstable, Combine and Connect, and were thus not included in subsequent analyses.

Of the six stable topics, four were related to cybersecurity assertions and two were not. Table 2 provides information about the cybersecurity-scaling relationship by identifying the six stable topics and the cybersecurity assertions that were related to them. Seven cybersecurity assertions were related to Position, two to Innovate, one to Fundraise, and one to Complement. In total, 11 cybersecurity assertions were related to four stable topics.

Six cybersecurity assertions were considered not related to the topics shown in Table 1 because their topic loadings were less than 0.4. Table 3 provides these uncategorized cybersecurity assertions.

Table 2. Topic and cybersecurity assertion relationships



Topic	ID	Cybersecurity assertion	Loading
A. Fundraise	A044	Develop and implement a governance model to scale, raise capital, protect against the unauthorized use of electronic resources, and leverage business ecosystems	0.49
D. Enable	N/A	N/A	N/A
E. Position	A068	Invest in company cybersecurity that improves cybersecurity of all members of the company value chain	0.87
	A067	Incorporate cybersecurity investment into scaling master plan	0.73
	A083	Operate in regions with strong cybersecurity policy and legal frameworks	0.66
	A016	Attain stakeholder trust by improving cybersecurity of the company and the players it works with	0.65
	A066	Incorporate cybersecurity in value propositions	0.53
	A009	Apply processes that continuously improve the cybersecurity of the company as well as its offers, channels and resources	0.47
	A038	Continuously train individuals in cybersecurity so as to i) improve cybersecurity operations, and ii) positively contribute to the company's cybersecurity culture	0.45
F. Communicate	N/A	N/A	N/A
G. Innovate	A102	Strengthen cybersecurity attributes of products and services compared to competitors	0.51
	A042	Deliver products and services that offer convenience, cater to customer demands, are secure and offer excellent customer experience	0.48
H. Complement	A088	Perpetuate a company culture of scaling based on a strongly held and widely shared set of beliefs that include high growth ambitions, delivering new benefits to customers, embedding in ecosystems led by fast growth companies, keeping the company and those it works with secure from cyberattacks, attracting investment, exceeding high standards, continuous improvement, experimentation, iteration, learning, and short feedback loops	0.67

Discussion

The results suggest that what a new company does to scale company value rapidly can be organized into six topics labelled Fundraise, Enable, Position, Communicate, Innovate, and Complement. The results also suggest that what a new company does to protect against the malicious or unauthorized use of electronic data is related in four ways to what it does to scale company value rapidly.

First, to strengthen its position among members of the network upon which it depends to scale, a new company can invest to continuously improve the cybersecurity of the company and of the members of its value chain; operate in regions with strong cybersecurity policy and legal frameworks; incorporate cybersecurity into value propositions; and train its employees in cybersecurity.

Second, to deliver innovative products and services and improve value propositions, a new company can strengthen the cybersecurity attributes of products and services compared to competitors and commit to delivering products and services that are secure.

Third, to align benefits to customers, resource owners, and other key stakeholders, a new company can perpetuate a culture of scaling its value based on a strongly held and widely shared set of beliefs, which includes keeping the company and those it works with secure from cyberattacks.

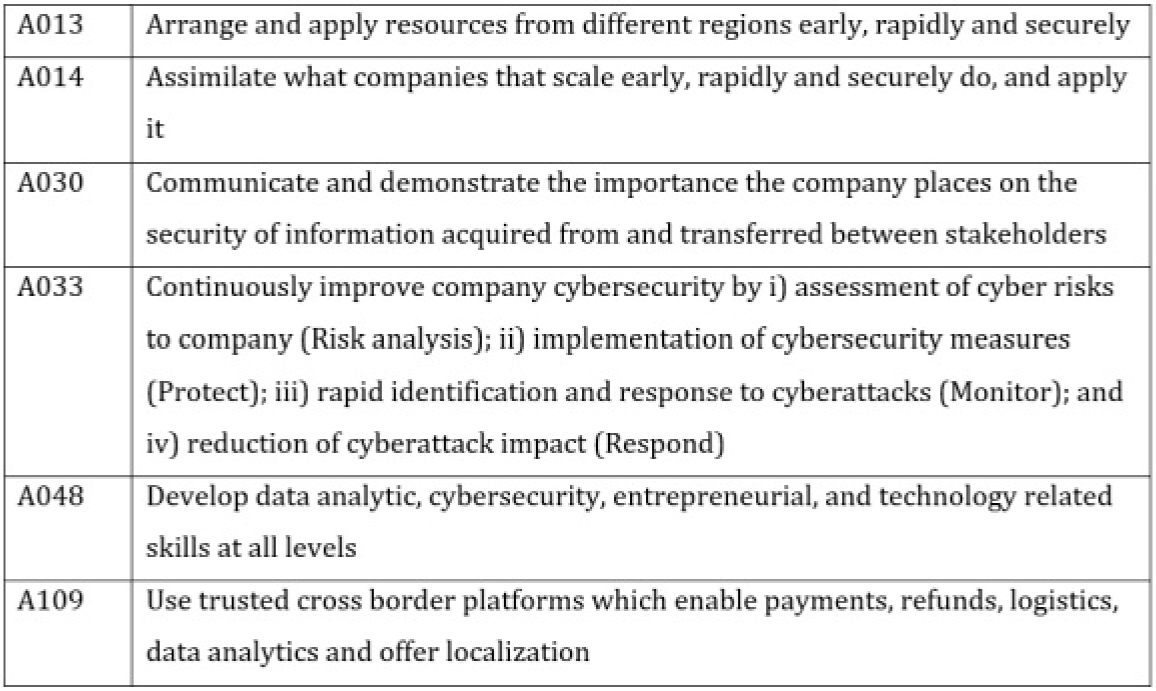
Fourth, to align returns to investors' capital with scaling opportunities, a new company can develop and implement a governance model that includes protecting against the unauthorized use of electronic resources.

Conclusions

The topic model results show that 11 cybersecurity assertions involving the scaling of a company's value are related to four topics: Position, Innovate, Complement, and Fundraise. Thus, what a new company does to protect itself and its partners against the malicious or unauthorized use of electronic data is related to what it does to scale company value rapidly in at least four ways. Our topic modelling reinforces the evolving professional and academic literature perspectives regarding cybersecurity as being a business enabler or influencer. The results certainly are contrary to cybersecurity being an innovation blocker.

While performing this analysis provided interesting perspectives on the cybersecurity-scaling relationship, it was a difficult path to follow. While running a topic model is fairly straightforward, to actually determine the

Table 3. Uncategorized cybersecurity assertions



A013	Arrange and apply resources from different regions early, rapidly and securely
A014	Assimilate what companies that scale early, rapidly and securely do, and apply it
A030	Communicate and demonstrate the importance the company places on the security of information acquired from and transferred between stakeholders
A033	Continuously improve company cybersecurity by i) assessment of cyber risks to company (Risk analysis); ii) implementation of cybersecurity measures (Protect); iii) rapid identification and response to cyberattacks (Monitor); and iv) reduction of cyberattack impact (Respond)
A048	Develop data analytic, cybersecurity, entrepreneurial, and technology related skills at all levels
A109	Use trusted cross border platforms which enable payments, refunds, logistics, data analytics and offer localization

optimal number of topics or which topics are stable was both labour intensive, and required judgement calls about how to make specific decisions on stability, or regarding the relationship strength of the assertions. One way forward is to develop techniques and associated automated tools that can facilitate the analysis of cybersecurity, both regarding selecting the number of topics and the topic stability analysis.

This paper increases our understanding of cybersecurity in the context of new companies that scale rapidly. The analysis showed that cybersecurity is strongly related to companies positioning themselves within networks for which the company is dependent for scaling, is an important component of company innovation, has linkages to fundraising, and supports the aligning of benefits to company stakeholders.

Dedication

Dan Craigen dedicates this paper to his late wife Elizabeth (Liz) Chung-Kin Chen-Craigen and to Dan and Liz's two daughters, Ailsa and Cailin, for their strength and encouragement.

Acknowledgements

We wish to sincerely thank Professors Michael Weiss and Stoyan Tanev of Carleton University's Technology Innovation Management program, Eduardo Bailetti, CEO of ScaleCamp, and Rahul Yadav, a graduate student in the Technology Innovation Management program, for their various contributions to this paper.

References

Bello, P. 2019. How cybersecurity accelerates business growth. *HelpNetSecurity.* October 21. https://www.helpnetsecurity.com/2019/10/21/cybersecurity-accelerates-business-growth/

Blei, D.M., Ng, A.Y. and Jordan, M.I. 2003. Latent dirichlet allocation. *Journal of Machine Learning Research*, 3 (Jan): 993-1022.

Blei, D.M., 2012. Probabilistic topic models. *Communications of the ACM*, 55(4): 77-84.

Blivet, C. 2019. *Why businesses need to rethink cyber security as a business priority.*

Boyd-Graber, J., Hu, Y. and Mimno, D., 2017. Applications of topic models. *Foundations and Trends® in Information Retrieval*, 11(2-3): 143-296.

Carney, J. 2011. Why integrate physical and logical security. *CISCO white paper.* https://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/pl-security.pdf

Cohen, P. 2019. Why cybersecurity is a business enabler. *F-Secure*, July 3. https://blog.f-secure.com/why-cyber-security-is-a-business-enabler/

Craigen, D., Diakun-Thibault, N., & Purse, R. 2014. Defining Cybersecurity. *Technology Innovation Management Review*, 4(10): 13-21. http://doi.org/10.22215/timreview/835

Emmerson, T., Hatfield, J.M., Kosseff, J. and Orr, S.R. 2019. The USNA's interdisciplinary approach to cybersecurity education. *Computer*, Volume 52, Issue 3, March.

Giever, D. 2018. Commentary: An argument for interdisciplinary programs in cybersecurity. *International Journal of Cybersecurity Intelligence & Cybercrime*, Volume 1, Issue 1.

Hampson, R. 2019. Making money from cyber security. *ETF Stream*. September 25. https://www.etfstream.com/feature/9262_making-money-from-cyber-security/

Kayworth, T. and Whitten, D. 2010. Effective information security requires balance of social and technology factors. *MS Quarterly Executive*, 9(3): 163-175.

Nelson, N. and Manick, S. 2017. Studying the tension between digital innovation and cybersecurity. *3rd International Conference on Information Systems Security and Privacy*, February. https://aisel.aisnet.org/amcis2017/InformationSystems/Presentations/31/

Orange, 2020. http://orange.biolab.si/widget-catalog/text-mining/topicmodelling-widget/ Accessed February 25, 2020.

Ramirez, R.B. 2017. Making cybersecurity interdisciplinary: recommendations for a novel curriculum and terminology harmonization. *Thesis, Master of Science in Technology and Policy*, MIT.

Singer, P.W. and Friedman, A. 2014. *Cybersecurity and Cyberwar: What everyone needs to know.* Oxford University Press.

Sloman, C. 2018. Reframing cybersecurity as a business enabler. *Innovation Enterprise*, April 18. https://channels.theinnovationenterprise.com/articles/reframing-cybersecurity-as-a-business-enabler

Softlanding. Accessed December 30, 2019. https://www.softlanding.ca/about-Softlanding/resources/blog/why-businesses-need-rethink-cyber-security-business-priority

Soomro, Z.A., Shah, M.H., Ahmed, J. 2016. Information security management needs a more holistic approach: a literature review. *International Journal of Information Management*, 36(2): 215-225, April.

Trott, D. 2019. Making Security an Enabler by Delivering Business Outcomes. *IDC*, May. https://www.orange-business.com/en/library/analyst-report/orange-cyberdefense-infobrief

Von Solms, R., and van Niekerk, J. 2013. From information security to cyber security. *Computers & Security*, Volume 38: 97-102.

Watson, R. 2019. How embracing cybersecurity can help your company's growth strategy. *EY.* July 25. https://www.ey.com/en_gl/advisory/how-embracing-cybersecurity-can-help-your-companys-growth-strategy

Xing, L. and Paul, M.J. 2018. Diagnosing and improving topic models by analyzing posterior variability. In *Thirty-Second AAAI Conference on Artificial Intelligence*, April.

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 past 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.

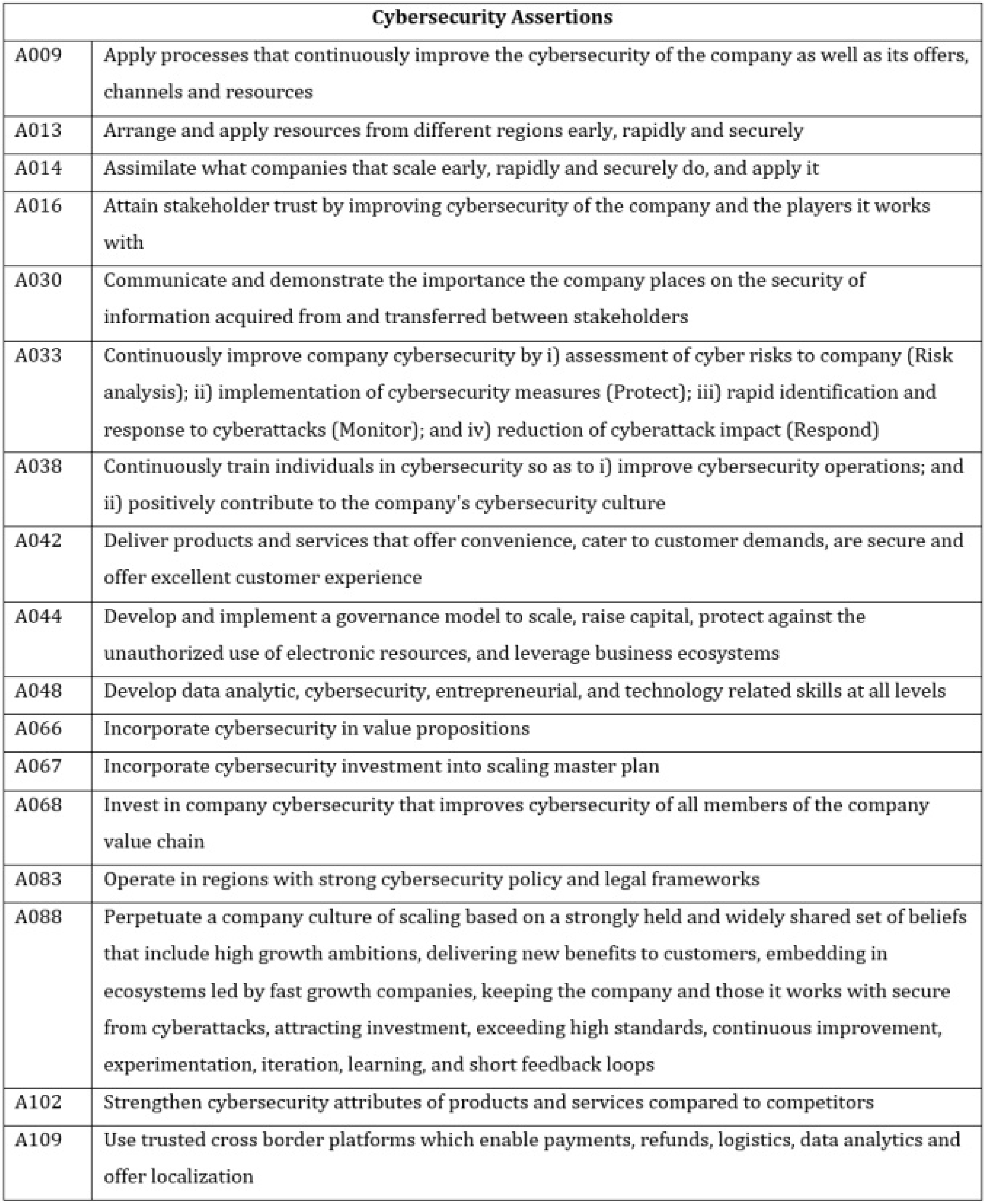
Mr. Craigen is the community and project manager with the Technology Innovation Management Program, Carleton University. Formerly, he was the Director of Carleton University's Global Cybersecurity Resource (GCR) (https://www.cugcr.ca) and was the founding president of Global EPIC (https://www.globalepic.org). Mr. Craigen was a senior science advisor with the Government of Canada for 12-years and President of ORA Canada, a company that focused on high assurance technologies and distributed its technology to sites in 65-countries. Mr. Craigen was the Chair of two NATO research task groups ("Dual use of high assurance technologies" and "Validation, verification and certification of embedded systems.") Mr. Craigen obtained a B. Sc (Honours Math) and an M. Sc from Carleton University.

Citation: Bailetti, T. and Craigen, D. 2020. Examining the Relationship Between Cybersecurity and Scaling Value for New Companies. *Technology Innovation Management Review*, 10(2): 62-70. http://doi.org/10.22215/timreview/1329

CC BY

Keywords: Cybersecurity, scaling company value, topic model stability, scaling initiatives.

Appendix A. Collection of 17 cybersecurity assertions



Cybersecurity Assertions	
A009	Apply processes that continuously improve the cybersecurity of the company as well as its offers, channels and resources
A013	Arrange and apply resources from different regions early, rapidly and securely
A014	Assimilate what companies that scale early, rapidly and securely do, and apply it
A016	Attain stakeholder trust by improving cybersecurity of the company and the players it works with
A030	Communicate and demonstrate the importance the company places on the security of information acquired from and transferred between stakeholders
A033	Continuously improve company cybersecurity by i) assessment of cyber risks to company (Risk analysis); ii) implementation of cybersecurity measures (Protect); iii) rapid identification and response to cyberattacks (Monitor); and iv) reduction of cyberattack impact (Respond)
A038	Continuously train individuals in cybersecurity so as to i) improve cybersecurity operations; and ii) positively contribute to the company's cybersecurity culture
A042	Deliver products and services that offer convenience, cater to customer demands, are secure and offer excellent customer experience
A044	Develop and implement a governance model to scale, raise capital, protect against the unauthorized use of electronic resources, and leverage business ecosystems
A048	Develop data analytic, cybersecurity, entrepreneurial, and technology related skills at all levels
A066	Incorporate cybersecurity in value propositions
A067	Incorporate cybersecurity investment into scaling master plan
A068	Invest in company cybersecurity that improves cybersecurity of all members of the company value chain
A083	Operate in regions with strong cybersecurity policy and legal frameworks
A088	Perpetuate a company culture of scaling based on a strongly held and widely shared set of beliefs that include high growth ambitions, delivering new benefits to customers, embedding in ecosystems led by fast growth companies, keeping the company and those it works with secure from cyberattacks, attracting investment, exceeding high standards, continuous improvement, experimentation, iteration, learning, and short feedback loops
A102	Strengthen cybersecurity attributes of products and services compared to competitors
A109	Use trusted cross border platforms which enable payments, refunds, logistics, data analytics and offer localization