Business modeling facilitated Cyber Preparedness

Julius Francis Gomes
Petri Ahokangas
Martti Ahtisaari Institute
Oulu Business School, University of Oulu, Finland

Kwadwo Atta Owusu
Department of Management and International Business
Oulu Business School, University of Oulu Finland

Acknowledgement: This study has been supported by the DIGILE Cyber Trust – Digital cyber security program.

Keywords
Cyber security, Cyber threat, Cyber preparedness, business model, competitive advantage, management model.

Abstract

Cyber criminality being one of the key threats in modern era lacks attention from academic perspective. In this paper, we display how to apply core business conceptual tool like business model to help improve organizational cyber preparedness. This paper offers a literature review and further analysis to find synergies among the study context and concept. Our findings of this initial paper supports the idea of applicability of business models in the cyber preparedness framework to gain organizational competitive advantage. Our analysis reflects on the content, structure and governance perspective which is professed in business model literature. Practical implication of this paper is that it offers security specialists with additional lens to look at how to approach more comprehensively the growing incidents of potential cyber threats. Cyber security related problems are not described in the literature as the way we display in this paper from a business and managerial perspective, which offers industry specialists fresh perspective for analysis.

1 Introduction

In February 2016, one of the biggest bank heist rocked the central bank of Bangladesh. Unknown hackers broke the security system of the bank and reportedly made away with $81 million from its account deposited at the Federal Reserve Bank of New York (NY Times 2016). In the course of the heist, 35 separate withdrawal requests amounting to $951 million was tried by the attackers (Reuters 2016). In commenting on the incident, the resigned governor of the Bangladesh Bank likened the cyberattack on the bank to a terrorist attack.

Cyber security is one major issue in industries like financial services, defense, healthcare, media and online social media (Dobrian 2015). Cyber criminality takes many faces, such as: digital piracy, fraudulent use of IPR (intellectual property rights), impersonation, phishing, blackmailing or extortion and many others. The most intriguing aspect of these activities is the exploitation of personal or in some cases organizationally confidential information in abusive manner. It is likely that in all cyber-crimes that took place, measures were taken to stop the bleeding. It is therefore imperative that both the academia and industry agrees on a preventive framework that can save the ICT dependent globe from being robbed in broad daylight in such ways.

Cyber-attacks are launched in many different ways. Most of them are launched solely from the external environment of the organization, though in some cases there are some insider

involvement observed. Birkin Shaw& Goddard (2009) identifies the two major question for a firm which concerns the actual business of the firm and the management dimension of the firm. These two perspective discusses both internal and external orientation of a firm. All of the cyber-attacks have strong foothold in organization's external environment. Having said that, it is thus important to study this external side along with the internal managerial side of the environment in order to have a better cyber prepared entity. In doing so, we use business model as a conceptual tool to explain the external part of the story.

In this paper we discuss the concept of cyber-preparedness (Bodeau, Graubart & Fabius-Greene 2010) that has already been in the literature for few years, however implementation at organization level might be questionable due to the limited explanation in literature and how challenging it can be to conceptualize for practical implementation. Furthermore, we present the concept of business modeling as a means to facilitate implementing organizational cyber-preparedness strategies. The explorative research question that we handle in this research is as follows:

How could business model facilitate organizational cyber-preparedness strategies?

Ever since the dot-com-boom during the 1990s, business model have emerged to be a buzz phenomenon in the ICT industry to trial different ways of conducting business. However, within the extant literature of business modeling, the essence of cyber threats have been less visible as a discussion point. This paper will help business readers understand the cyber threats and security issues. On the other hand, for cyber security experts this paper will provide insights about how business models can facilitate preparedness in the presence of cyber threats as an issue.

The rest of the paper is structured as follows. First, a brief discussion on how cyber-criminality and threats are perceived is presented, followed by a discussion on cyber-preparedness framework. Second, we present a comprehensive review on the concept of business model which is a comparatively new phenomenon in the field of cyber-security. Finally, we discuss how business modeling could enhance cyber-preparedness framework implementation.

2 Context

Cyber threat and cyber crimes

The advancement in knowledge, science and technology is driving change in the globalized world (Lehto 2013). This development has made companies to rely on information technology in almost every aspect of their operations or functions. Not only do firms use IT in their internal operations, they also employ it in their external operations. For instance, a firm can use internet-based applications to coordinate its supply chain activities. In other words, firms leverage advantages that the IT brings to enhance their efficiency and increase their productivity.

Just as businesses want to leverage the benefits of the cyberspace to enhance their productivity, there are equally other actors who also would want to use the cyberspace for malicious purposes. This malicious motive open up businesses to diverse vulnerabilities and threat of cyber-attack. Cyber threat can be defined as an event or the deliberate exploitation of vulnerabilities by threat agents or attack vectors leading to the disruption in an organization's operations, or the loss or takeover of an organization's assets (Lehto 2013). The threat to organization's assets like information and IT infrastructure may arise from natural occurrence like earth quake, equipment failure or unintentional actions of employees. However, the deliberate, planned attack that poses the highest risk and is able to wreak incalculable loss to organizations is of interest in this paper.

Types of Cyber Threats

Cyber threats are classified differently in the literature but the one most used is the model that classifies cyber threat on five levels based on the motivational factors of the threat agents (Bodeau et al. 2010; Lehto2013). These are cyber activism, cybercrime, cyber espionage, cyber terrorism and cyber warfare.

Cyber activism is the first level of threat and it entails cyber vandalism, the so-called 'hacktivism', and hacking. The intent of these actors may not be to cause any damage but may be using the attack to embarrass an organization or send a political message (Bodeau et al. 2010; Vatis 2002). 'Hacktivists' are individuals or groups who hack into publicly available websites and overload email servers to send a politically motivated message or use it to convey a protest message, for example, against limiting civil liberties (Lehto 2013; Vatis 2002). Examples of these groups are Anonymous, Teampoison, ChaosComputer Club (Raza 2016).

The second level of threat is cybercrime. It involves the use of information systems and networks by adversaries for the commission of crime against a victim's IT infrastructure. This act can be perpetuated by individuals or loosely-organized groups, terrorists, insiders or spammers. The motive for this attack could be the stealing of vital information, disrupting the functions or operations of organizations for financial gain or ideological cause (McCuster 2006; Valis 2002). According to Lehto (2013), cybercrime can be categorized into three groups: the use of ICT to commit traditional crimes like fraud and forgery; the publishing of illegal material over the electronic media; and attacks directed at the electronic network.

Cyber espionage is the next level of threat. It is the use of illegal means on the internet or networks, programs or computers to get secret information from individuals, organizations, competitors, and governments for political, military or monetary gain (Liaropoulos 2010; Lehto 2013). Cyber espionage is carried out by professional intelligence agents, individuals or groups who exploit the vulnerabilities in their adversary's system in order to get high-value information. It is a tactic employed by nation-states and their militaries to gather intelligence on their perceived or real enemies (Bodeau et al. 2010; Valis 2002). Cyber espionage is not limited to political espionage, but it extends to economic domains. Professional organized crime group or agents of an organization's competitors can hack into a business entity's system and steal their proprietary information like intellectual property and trade secrets. A classic case is the alleged stealing of a US wind turbine software designer, AMSC's code by a Chinese wind turbine manufacturer, Sinovel (Fortune 2015).

The fourth level of threat is cyber terrorism. It is the use of cyber-attacks targeted at IT systems or critical infrastructure of government and private organizations with the intent of intimidating a government or causing fear and panic among civilian population (Valis 2002). This attack is perpetuated by sophisticated terrorist groups whose aim is to grab national or international attention (Beggs 2006). They utilize offensive IT weaponry either in isolation or in combination with other means of attack (Lehto 2013). For example, in 2011, the Canadian government reported a major cyber-attack against its agencies, including Defence Research and Development Canada. The attack forced the Finance Department and Treasury Board, Canada's main economic agencies, to disconnect from the Internet (NATO 2013).

Cyber warfare is the fifth level of cyber threat and it involves the conduct of warfare in the virtual world or cyberspace (Lehto 2013). The typical threat agents are nation-states' military and their intelligent services, organized insurgent groups or terrorists. The action aims at immobilizing the information system or destroying critical infrastructure of the enemy through the use of weapons like computer viruses, worms or denial of service attacks (DOS). Cyber warfare is not a standalone strategy but it is used with other strategies (e.g. 'kinetic' warfare) in an offensive or defensive operation (Bodeau et al. 2010). For example, in 2007 the Estonian

government suffered some serious cyber-attacks against its websites and some banks' websites leading to a halt in online banking transactions. This incident arose when the government decided to relocate a WWII Soviet Union memorial (Herzog 2011).

The forgoing discussion has centered on the various types, levels of severity and complexity of cyber threats. The threat can emanate from various sources like nation-states, organizations, organized crime groups, individuals, terrorists, insurgent groups and competitors. The motive of these actors may be to enhance their ego or have some bragging rights, to advance a political or ideological cause, for monetary gain, to get access to sensitive information for a future course of action, to cause fear and panic among people or to force a government to take or abandon a certain cause and used as a strategy in conflicts and warfare. The severity of these attacks may differ from one another and the intent may be to cause minimal or collateral damage. Nevertheless, in all instances, a cyber-attack result in some form of loss, such as: financial loss, infrastructure or equipment damage, and loss of reputation. In the next section, we examine the costs of cyber-attacks to nation-states and businesses.

The cost of cyber attacks

The incidents of cyber-attacks are increasing with a concomitant increase in cost to governments and businesses. The actual cost of these attacks is difficult to quantify, however numerous studies have churned estimated costs (Ulsch 2014). According to Lehto (2013), the average annual cost of cyber-attack to US organizations was US$8.9 million and the cost of solutions used in preventing denial of service attacks is anticipated to reach US$ 870 million by 2017. Similarly, the cost of cybercrime to the US ranges between US$ 24 billion and US$ 120 billion and the global cost is reported to be US$ 1 trillion (Fortune 2015). Also, the Intellectual Property Commission estimates that the US losses around US$ 300 billion annually through intellectual property theft. In a recent study of 58 benchmarked US organizations, the Ponemon Institute found that the average cost of cybercrime to these organizations was US$ 15 million. This showed an increase of 19% in the 2014 survey figure (Ponemon 2015).

The cost of cyber-attack can be broadly divided into two: preventive cost and post attack cost (Ulsch 2014). The preventive cost is investing in infrastructure and systems, for example, to reinforce the perimeter defense of an organization to prevent an intrusion or reduce the impact of a breach. Although the cost of preventive solutions may be high, it may not be as expensive as the post attack remedies. The post attack cost involves the actual cost (e.g. monies stolen and extortion) and the cost of measures to remedy the consequences of the attack. This includes the cost of replacement or repair of damaged infrastructure or systems; cost of repairing lost business such as customer acquisition activities and image rebuilding efforts; and cost of detection and reporting like forensic and investigative activities, audits of installation and systems, crisis management and communication to stakeholders (Ponemon 2015).

The dependence on the cyberspace by businesses to conduct their functions and business transactions leaves them vulnerable to the risk of cyber-attacks. Just as organizations cannot avoid the use of the interconnected electronic space because of these inherent threats, they can institute measures to minimize their vulnerability. These measures include developing a proactive strategic and operational preparedness plans that they can fall on to thwart potential or actual cyber-attacks. We now move the discussion to cyber preparedness

Cyber preparedness Framework

Businesses are aware of their vulnerabilities to cyber-attack. Some expose themselves and only react when they are attacked. Others that appear proactive leave the task of protecting their organizations systems and IT infrastructure to their security managers (Scully 2014). This adhoc

approach to managing cyber risk exposes businesses to cyber-attack and its attendant consequences (EY 2015).

Cyber preparedness is the deliberate institution of cyber security preventive measures targeted at the dynamic vulnerabilities and cyber threats businesses constantly face. It is a policy issue and needs to evolve from an organization's leadership and cascade down to the whole organization. A comprehensive framework that can help organizations to develop cyber preparedness policy has been proposed by Bodeau et al (2010). This framework adopts a four stage methodology in crafting the strategy. In the first stage, leadership lay out its approach to business risk management; in the second stage, the level of preparedness is determined; the third stage involves the analysis of the organizational capabilities to support its preparedness; and the final stage entails the development of roadmap and integration into the strategic plan (Bodeau et al. 2010).

In the first stage, the leadership examines the organization's threat levels, the existing security risk management frameworks to guide strategy formulation. The levels of threat correspond to those already enumerated in the discussion. At the lower levels, the motive of the attack is for short term benefits so the organization strategies are fashioned to keep intruders out or to neutralize their attacks expeditiously. At the higher levels the intent of the actors is to undermine an organization's raison d'état so the strategies are geared towards the design of robust systems and business functions of the organization (Bodeau et al. 2010).

In the next step, leadership critically assesses it cyber preparedness level in relation to the threat levels identified. The cyber preparedness levels are: *perimeter defense, critical information protection, response awareness, architectural resilience and pervasive agility* (Bodeau et al.). At the lower levels the organizations goals may be to prepare for known external attacks, to prevent unauthorized access to sensitive information or information infrastructure. The possible strategies employed at this level are: using perimeter defense mechanisms to protect the information system; employing encryption, access control methods to protect critical data and deploys capabilities to identify and respond to penetration attempts. At the higher levels, architectural resilience and pervasive agility strategies are adopted preventing limiting attacks, contain and recovering from successful attacks of adversaries (Bodeau et al.).

In the third stage, the organization evaluates the nature of the threat it faces and its technical, operational and process capabilities at its disposal to mitigate the threat it faces. To be able to deal successfully with a threat, the organization has to be abreast with the capabilities, intentions and targeting activities of the actors. An organization's knowledge of the tactics, techniques and procedures (TTPs) an adversary is likely to deploy will keep them ahead in thwarting the attack. Having armed itself with the nature of the threat, the organization then deploys its technical and operational arsenal to prevent or stop the threat. Examples of these solutions are perimeter firewalls, encrypted external transmissions between internal and trusted external systems, honeypots, insider monitoring and penetration testing of physical security of organization's facilities.

Having developed the cyber preparedness policy, the final step entails the drawing a roadmap to integrate the policy into the overarching strategic plan. The implementation of the cyber preparedness plan involves expense at each level of preparedness, therefore top management need to carefully plan the implementation timelines, provide the resources for the implementation and remove any bottlenecks (Bodeau et al. 2010).

3 Theoretical framework

The two most important questions that an organization needs to find answer in order to operate successfully involves asking what is the actual business of the firm and how do they manage the organization (Birkin Shaw& Goddard 2009). This two questions shows the two sides of the story, the internal management logic and the external business logic.

In this section a conceptual review of the business perspective is presented by studying business model. Then a brief note about organizational management dimensions provides further grounding to analyze cybersecurity issues through these lenses. It is arguable that defining what business an organization is in, how they manage the business, how they manage the organization as an entity and how all of these converge can help a company to better prepare against cyber threats.

Business Model

What business the specific entity is in is perhaps the most valuable question that is to be defined. Since it enquires mostly about external activities of a firm, we review the concept of business model as the key to explain a business. The answer to what business a firm is in might be simple and too straight forward, but to understand the overall "business" logic of a specific firm's business model as a tool explains all the "business" related activities but not management related ones.

Business model as a research interest has had its root in Information Systems since the late 1970s (Wirtz 2010). During the early stage of business model research, it was concerned almost entirely for e-businesses and Internet based businesses in the post-dot-com-boom era. However, in recent years, research on business model has grown to explain business logic from more generalized perspective and not only specific contexts. Additionally, although business model had its roots in IS no significant research work on cyber security and threats is offered harnessing the potentials of the business model concept. Due to the lack of application of business models in the cyber security context, it is ideal to visit some of the most widely acknowledged definitions of the concept.

Timmers (1998) described business models to be the *architecture* of product, service and information flows, including a description of the various business actors and their roles. He added it to be a description of the likely benefits for a range of business stakeholder and a description of the sources of revenues. On the other hand, Weill & Vitale (2002) generalizes the concept to be *roles and relationship* among a firm's consumers, customers, allies and suppliers that identifies the major flow of product, information and money, and the major benefits to participants.

Morris, Schindehutte& Allen (2005) identifies business models to be concise representation of how an *interrelated set of decision variables* in the areas of venture strategy, architecture and economies are addressed to create sustainable competitive advantage in defined markets. According to Shafer, Smith & Linder (2005), it is a representation of firm's underlying *core logic* and *strategic choices* for *creating and capturing value* within a value network. Amit &Zott (2001) defines the business as to depict the *content, structure, and governance* of transactions designed so as to create value through the exploitation of business opportunities. Considering that transactions connect activities, the authors further evolved this definition to conceptualize a firm's business model as a *system of interdependent activities* that transcends the focal firm and spans its boundaries (Zott& Amit 2010).

In the extensive business model literature, besides defining the jargon, researchers have endeavored to offer different meta-modeling tools with structured elements. Osterwalder, Pigneur&Tucci's (2005) *Business Model Canvas* is one of the most popular tools which specifies

nine different elements to be considered while creating a specific business model for a firm. These elements are: value proposition, customer segments, customer relationship, channels, key partners, key activities, key resources, cost structure and revenue stream. Ahokangas, Juntunen&Myllykoski's (2014) *Business Model Wheel* is another action oriented and opportunity centric tool which is gaining significant traction lately in practice. Building on Onetti et al's (2012) approach to consider the focus, locus and modus of a business; Ahokangas et al (2014) uses what, how and why questions regarding the business. Elements that the business model wheel answers include customer types, offering, value proposition, differentiators, sales and marketing, mode of delivery, basis of competitive advantage, key operations, basis of pricing, way of charging and cost elements.

Focusing on different specific elements that business model meta-modeling tools offer might seem to be more relevant for a case when identifying "business logic" is the core purpose. Since in this research we tend to find how the concept fits while preparing an entity against cyber criminality, we find it justifiable to first contemplate on the phenomenon more from a conceptual level. By doing so, we can find the feasibility of applying the business model phenomenon in the cyber security context, since it is not done currently. In practice, once the applicability of business models in cyber preparedness seem feasible, different meta-modeling tools can be used by companies.

Reflecting back to the definitions of business model from the literature a holistic stream can be identified. Combining all of the definitional perspectives presented above we see business model as an architectural (Timmers 1998) system of interdependent activities (Zott& Amit 2010) and interrelated set of core logic & strategic decision variables (Morris et al. 2005; Shafer et al. 2005); explaining transaction content, transaction governance and transaction relationship structures (Amit & Zott 2001; Weill & Vitale 2001).

In practice, organizations need to orchestrate number of activities in order to execute functionalities. These activities are often interdependent which also has some impact on the inner half of the organization as well. Usually, these activities should be synergized in a way to reflect the core purpose or logic of the firm's business and move forward by implementing organizational strategic choices. All of these activities should then explain the content, structure and governance (Amit & Zott, 2001) of each transaction. Amit & Zott (2001) refers to the goods and information that is being in play as the transaction content, additional to the resource and capabilities to complete the exchange. Transaction structure describes the parties involved in the process and the sequence of their participation. Also it explains the adopted exchange mechanism for completing an exchange influencing adaptability, flexibility and scalability. Finally, transaction governance refers to the control protocol of information, resource and goods flow by relevant parties.

The business model concept has been reviewed from a conceptual perspective in this research. Going forward we study the inner half of an entity. The conceptualization from this section will be later used to analyze how business modeling should be in the time of cyber threats and how business models can eventually facilitate cyber preparedness of an organization.

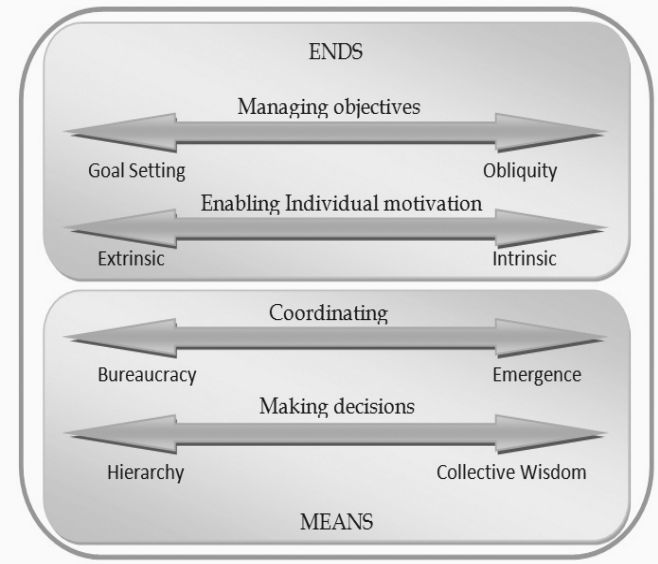
Management dimensions

Having answered what the firm's business is and how the business is managed, the next vital question to be answered is how the organization is internally managed. We reflect upon Birkin Shaw& Goddard's (2009) framework for dimensionalizing management. The reason to reflect upon such concept is because it deals with organization's most fundamental level choices to shape specific behaviors and practices within a firm. Also, by understanding the managerial

alternatives, it is possible to apply conscious changes to improve competitiveness. Though there is no single best management model for every firm, it is vital that alternative models serve as a pool of choices to choose in different situations and in different contexts.

From a management perspective, organizations have managerial goals or ends and there are means to achieve those managerial ends. Birkin Shaw& Goddard two major organizational ends, they are: managing objectives and enabling individual motivation. On the other hand, means to achieve ends are also classified into two types, they are: coordinating activities and making decisions. For each of these four means and ends Birkin Shaw& Goddard identified two polar extremes to map how specific management model can be. Figure 1. Summarizes the framework of management dimensions.

For managing objectives, organizations can have preset and determined goal and sub-goals or objectives that they want to achieve in order to achieve the greater goal. Alternatively, some organizations can improvise based on the existing market situating in order to achieve ultimate goal. To motivate individuals, rewards can be either extrinsic or intrinsic, such as, monetary benefits or sense of achievement respectively. As for means to achieve the managerial ends, coordination of organizational internal and external activities is important. Such coordination can be done in a standard bureaucratic manner or organizations can encourage emergence by avoiding unnecessary bureaucracy. Finally, there are such organizations where final decisions are



made by superiors without consulting or considering actual personnel's involved in operation. In such cases superiors usually take direct accountability and authority; however the decisions are executed by subordinates. The alternative is a collective intelligence scenario where decisions are made collectively by consulting with operational personnel.

Figure 1. *A framework for dimensionalizing management (Adapted from Birkinshaw& Goddard 2009).* Birkin Shaw& Goddard's framework offers a space to build an array of multitude of management models for different companies. Since there is no single best management model, it depends on the organizational management what model they want to adapt and how do they want to manage the firm. When thinking of building a model, management need to consider all of the four means and ends. It is then important to identify on which side of the extremes the organization wants to see itself to be productive, efficient, profitable, sustainable and secure most of all as the focus of this research.

4 Business model facilitated cyber preparedness

The huge figures presented as cost of cyber-attacks can have serious economic, reputational, competitive and survival repercussions for organizations. Considering such issues on the line, it is imperative organizations need to develop policy frames to deal with cyber-attacks. We perceive that business model as a conceptual tool can be applied to structure overall -business operations of the firm in synchronization of the management dimensions of a firm.

Current literature identifies cyber threats arising in the form of cyber vandalism, cyber theft, cyber incursion/surveillance, cyber-sabotage/espionage and cyber warfare. All of these cyber security issues involve the external environment of the entity. Although in some cases certain insiders play a role, outside dominance stays more pervasive. In the light of this, cyber preparedness strategy that ignores external links of the entity seems not only illogical but also reckless.

Bodeau et al's four stage methodology towards cyber preparedness appears logical. Yet, there is room to make the framework more complete. We attempt to do so by looking at how the cyber preparedness methodology framework fits with the business model and management dimensionalizing perspectives. Table 1. Reflects the summarizes how these two conceptualizations can be brought together.

Cyber preparedness methodology framework steps	Business Model/ Management mode perspective
Approach to manage business/organizational risk	Management objective / Ends
The level of preparedness	Preparedness content
Analysis of organizational capabilities	Preparedness structure
Roadmap & integration into a strategic plan	Preparedness governance

Table 1. *Combining cyber preparedness with business model and management dimensionalizing perspective. (Adapted from Bodeau et al 2012, Amit &Zott 2001, Birkinshaw& Goddard 2009)*

Towards organizational cyber preparedness, management needs to identify first their approach to manage business and organization risks. This obviously can be perceived as a management objective/end (Birkin Shaw& Goddard 2009). The rest of the three steps in the preparedness framework can be considered though as means to achieve the security objective. When defining the level of preparedness, organizations identifies the type of potential cyber-attacks that the firm might be under in certain contexts. These levels of preparedness can be perimeter defense, critical information protection, responsive awareness, architectural resilience and pervasive agility (Bodeau et al. 2012). From business modeling perspective, this stage can be considered as to be the preparedness content. Further in analyzing organizational capabilities, it involves assessing firm's internal operations, activities, resources, external networks of partners, competitor network, customer relations and also channels (Osterwalder et al. 2005, Ahokangas et al. 2012). While doing this, it resembles the tone of "transaction structure" quite closely, thus this can also be perceived as preparedness structure. Finally, roadmap & integration of cyber preparedness policy into a strategic plan can be considered to be the cyber preparedness governance plan (Amit &Zott 2001).

From a general perspective, the similarity between these frameworks perhaps appear to be only on conceptual level. However, looking carefully at the overall scene it can be observed that business model as a conceptual tool brings additional structure to the cyber preparedness framework by identifying specific objects which needs to be security checked or secured. Looking at the cyber security phenomenon from the content, structure & governance (Amit &Zott 2001)

perspective of business model, it can be argued that if we can strictly identify what type of security are we looking for (content), what and where do we need security (structure), how do we execute the overall security (governance) and how the overall organization is managed (Birkin Shaw& Goddard 2009), then the overall organizational cyber preparedness policy will be more comprehensive by not avoiding any vital variable that should be considered.

5 Conclusions

Security is such an essence in the modern technology dependent business world which is expected to come as a bundle offer with the product offering in most cases. This is more applicable for the consumer market than the B2B market due to the fact that business entities are concerned about corporate information and organizational confidential information. Albeit, Business model as a conceptual tool can be applied to invent new service/product concepts which will bring additional revenue to organizations for B2B setting. However, on a more general perspective bypassing revenue generation as the core, this paper looks to find how business model can play a role in preparing an organization against devastating cyber-attacks. We perceive cyber preparedness as to be the preventive measure based policy frame which is preferable than a post-apocalyptic recovery procedure.

Our brief analysis on how cyber preparedness and business model as a concept can be combined provides with some working conclusions. They can be treated as hypotheses based on literature review needing further empirical testing and refinement. From cyber security perspective, this literature review based paper offers interesting insight about how to approach it in practice and what sort of variables should be considered to safeguard a firm from potential attacks. On the other hand, for business model enthusiasts, we applied the business model concept to explain a phenomenon which is not directly revenue initiator. Given that under a security attack organizations are almost certain to lose financially or when securing against such attack, cyber security appears to be a cost incurring element for most players in industry. However, we take the concept of business model beyond revenue generation to improve organizational competitiveness. This leads to identifying competitive advantage for an organization by using business model as a facilitator for cyber preparedness.

The practical implication of this study would be offering security specialists with additional lens to look at how to approach more comprehensively to a growing incidents of potential cyber threats. From academic perspective, we display a way of conceptualizing the business model theory as a unit for analyzing organizational content, structure and governance for gaining competitive advantage by improving cyber preparedness. Most business model researches enlighten the literature by discussing value creation and value capturing logic. It is conceivable that security itself is a core value for customers regardless of the fact that it appears to be less sellable at the moment to consumers.

This paper can be considered to be a literature based conceptual discussion which opens up avenue for further research on the same topic and by empirical testing. There are hypothetical elements in our analysis, further empirical testing can validate such stands. Going forward, further research can also be done on how to capitalize on the competitive advantage that is brought by using business models facilitating cyber preparedness and how to monetize or create new revenue generating businesses for both B2B and B2C markets.

This paper is limited to the scope of literature surveying. Since the concept of cyber preparedness is so little explained in the literature and business models are also almost absent is cyber security context in the literature, we used this gap to organize the paper based on literature for this first paper of a coming series of publication. However, since the overall research on this

topic is still in nascent stage, we attempted for conceptual clarification and not empirical testing at this stage. Another limitation of the study was the lack of existing literature that concerns cyber security from a business perspective. From an originality perspective, this paper offers fresh way to look at a threatening phenomenon and the working conclusions appears to be promising for further testing.

References

Ahokangas, P., Juntunen, M. and Myllykoski, J., 2014. Cloud computing and transformation of international e-business models. A Focused Issue on Building New Competences in Dynamic Environments (Research in Competence-Based Management, Volume 7), Emerald Group Publishing Limited, pp.3-28.

Amit, R. and Zott, C., 2001. Value creation in e-business. Strategic management journal, 22(6-7), pp.493-520.

Beggs, C., 2006. Proposed risk minimization measures for cyber-terrorism and SCADA networks in Australia. In Proceedings of the 5th european conference on information warfare and security (ECIW 2006, Helsinki). Academic Publishing, Reading, UK (pp. 9-18).

Birkinshaw, J. and Goddard, J., 2009. What is your management model?.MIT Sloan Management Review, 50(2), p.81.

CNN, 2016, 'Bangladesh bank says hackers tried to steal $951 million', CNN Phillipines, Available from: http://cnnphilippines.com/business/2016/03 /14/Bangladesh-Bank-money-laundering-Philippines.html. [14 March 2016].

Dobrian, J., 2015. Are you sitting on a cyber security bombshell?.Journal of Property Management, 80(5), pp.8-12.

E.Y., 2015, 'Cyber preparedness: the next step for boards', Available from: http://www.ey.com/GL/en/Issues/Governance-and-reporting/EY-cyber-preparedness-the-next-step-for-boards, [21 March 2016].

Herzog, S., 2011. Revisiting the Estonian cyber attacks: Digital threats and multinational responses. Journal of Strategic Security, 4(2), p.49.

Kappos, D. J., &Passman, P., 2015, 'Cyber Espionage Is Reaching Crisis Levels', Available from: http://fortune.com/2015/12/12/cybersecruity-amsc-cyber-espiona ge/, [21 March 2016]

Lehto, M., 2015. Phenomena in the Cyber World. In Cyber Security: Analytics, Technology and Automation (pp. 3-29). Springer International Publishing.

Liaropoulos, A.N., 2011. War and ethics in cyberspace: cyber-conflict and just war theory. Leading Issues in Information Warfare & Security Research, 50.

McCusker, R., 2006. Transnational organisedcyber crime: distinguishing threat from reality. Crime, law and social change, 46(4-5), pp.257-273.

Morris, M., Schindehutte, M. and Allen, J., 2005. The entrepreneur's business model: toward a unified perspective. Journal of business research, 58(6), pp.726-735.

NATO, 2013, 'The history of cyber-attacks - a timeline', Available from http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm, [21 March 2016].

NY Times, 2016, 'Bangladesh Bank Chief Resigns after Cyber Theft of $81 Million', New York Times, Available from: http://www.nytimes.com/2016/03/16/ world/asia/bangladesh-bank-chief-resigns-after-cyber-theft-of-81-million.html? partner=rss&emc=rss&_r=0, [15 March 2016].

Onetti, A., Zucchella, A., Jones, M.V. and McDougall-Covin, P.P., 2012. Internationalization, innovation and entrepreneurship: business models for new technology-based firms. Journal of Management & Governance, 16(3), pp.337-368.

Osterwalder, A., Pigneur, Y. and Tucci, C.L., 2005. Clarifying business models: Origins, present, and future of the concept. Communications of the association for Information Systems, 16(1), p.1.

Ponemon Institute, 2015, 'Cost of Data Breach Study: Global Analysis. Report.', Available from: nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.PDF, [21 March 2016].

Raza, A., 2016, '10 Most Notorious Hacking Groups', Available from: www.hackread.com/10-most-notorious-hacking-groups, [21 March 2016].

Reuters, 2016, 'Bangladesh bank says hackers tried to steal $951 million', Reuters, Available from: http://www.reuters.com/article/us-bangladesh-bank-idUSKC N0WF0IL, [17 March 2016].

Scully, T., 2014. The cyber security threat stops in the boardroom. Journal of business continuity & emergency planning, 7(2), pp.138-148.

Shafer, S.M., Smith, H.J. and Linder, J.C., 2005. The power of business models. Business horizons, 48(3), pp.199-207.

Timmers, P., 1998. Business models for electronic markets. Electronic markets, 8(2), pp.3-8.

Weill, P. and Vitale, M., 2002. What IT infrastructure capabilities are needed to implement e-business models?.Mis Quarterly, 1(1), p.17.

Ulsch, N. M., 2014, 'Cyber threat! how to manage the growing risk of cyber attacks', [Books24x7 version] Available from: http://common.books24x7.com/toc.aspx?boo kid=63 511, [20 March 2016].

Vatis, M., 2002. Cyber-attacks: Protecting America's security against digital threats. Discussion pa.

Wirtz, B.W., 2010. Business model management. Gabler, Wiesbaden.

Zott, C. and Amit, R., 2010. Business model design: an activity system perspective. Long range planning, 43(2), pp.216-226.