STAYING AHEAD IN THE CYBER SECURITY GAME: WHAT MATTERS NOW

Mohammed ISHMEAL[*]

Erik van Ommeren, Martin Borrett an Marinus Kuivenhoven.(2014). Staying Ahead in the Cyber Security Game: What Matters Now: Sogeti and IBM.

The book as its title suggest stays ahead in the game of cyber politics tacitly and succinctly brings to bear concern issues relevant today and tomorrow. Although the authors of this work hinted the world in 2014, the expected challenges of cyber security in a complex cyber space world as information and computer technology evolutionalized, the solutions they provided in this premier book was quiet revealing and relevant to today's problems. In obvious expositions laid in a simple diction, the book analysis organizational security problems in the cyberspace taking into considerations management, usages and administration devoid of any form of technicalities detailed in the book. Thus, making cyber security a germane subject of enquiry in a capitalist world of business where security risk organizations profit is worthy of attention. The authors advocate states, organizations and individuals to transcend the technical area of information technology to consider social, economic, and ideological and the political dimensions. This is necessitated by the volume of increase in new computer devices, big data, software and the complex mobile usages by employees. In fact there is an imminent impact which poses security threats. In a 14 chapter discussion, the book presents each chapter independent of the other concentrating on the specific issue in relation to recent, relevance, solution and guiding principles.

The chapter one opens with a basic definition of Cyber security as "a set of people, process and technical practices aimed at protecting critical infrastructures, digital business and sensitive information from internal and external threats or negligence" (P, 15). Interestingly, despite the broad nature of the definition the authors discusses only a section of business organization. The emphasis of cyber security should rather be focused on protecting businesses and the society where interaction takes place. The credibility and sustenance of any business transaction hinges on how secured parties feel. Thus, the question of trust of people, the security of the organizations and benefit parties accrue occupies the central part of the three page discussion in this chapter. It is worthy to mention that the internet realm lacks

[*] PhD candidate at Selcuk University in the Department of International Relation, Konya, Turkey. Can e accessed via blkqatari@gmail.com

any coordinated concerted effort which could normalize the maladjusted system of the internet virtual world. Security had not been part of the responsibilities of the designers of the internet. In a fast developing virtual world where users become more sophisticated in a very fast pace, out-maneuvering the available technology is a threat to the very purpose of the relevance of Information Technology (IT). Obviously, the concern of security executives over clouds and mobile security were discussed as a shift of conventional security of IT has assumed much more public debate today. In fact recent activities where security experts such as John McAfee mobile and twitter account hacked[17] vindicate the authors of this book. The lesson is that no one is safe. As a result "pursuit of strategic advantage" (p. 17) in search of equilibrium between the hacker and the defender should be prioritized.

As they advocated for insightful and meaningful research to build a strong internet security structure, the chapter two, basically, advances the battle of the fitters in this unguarded cyber field of chaos where the "good" and "bad" guys compete for survival. Hacktivism from state to non-state actors and organized groups to individual criminals are scrambling for most lucrative element which is DATA, to advance their interest which could in blackmail, theft and conspiracy. In such a contested realm privacy and security becomes the *Janus* of the field of internet security.

The issue is that even when security officers possess the potential to protect and provide security to prospective victims their privacy remains an issue. This is so because, ethically, the security providers need the authorization of the individual before accessing his/her data. Thus, although privacy and security strive to protect, yet, it breaches on the confidentiality of the other. This issue of data ownership is well articulated at page 21 of the book. Fundamentally, the wishful list of cyber security officers from "securing end-to-end communication "developing "smarter system" and "a way to communicate to users about security" have improved not only the awareness of users but attempted to mitigate the level of attack. As is provided in the *Cyber Security Manifesto* "Keeping the flow of information running freely is an economic imperative". (P, 20).

Chapter three questions the difficulty in relation to employer-employee conflicting rights to usage and protection. How do we then restrict people's rights to using their preferred devices

[17] Joe Pinkstone *Mailonline* , " 'I have haters I am a target' Cybersecurity guru John McAfee goes on Twitter rant after claiming his accounts was hacked to promote vital currencies". 29th Dec, 2017 http://www.dailymail.co.uk/sciencetech/article-5220579/Security-guru-John-McAfees-Twitter-account-hacked.html

at work places at the expense of the organizations? Clearly, to protect the network system of institution there should be a choice of device provided by to people at the organization for the purposes of limiting the risk of being hacked. Chapter four therefore admonishes organizations not to limit security to technical or IT experts but should involve public relations officers, legal luminaries, human resource personnel, business expert, managers, political and economic experts. Cyber Security should therefore be a multi-facetted approach by all groups in relation to the business organization.

The chapter five argues that in designing software, apps and any form of internet device security should be incorporated to minimize insecurity and strengthen confidentiality and boost privacy. This approach is called security-by-design where the authors vividly provide carful explanations on the advantages and disadvantages to project. The authors argue that the "concept has far-reaching consequences and results"(P, 39). However, the chapter six identifies security measures through implementation convincing technologies as a way of default to regulate users' interaction with any form of technology in the virtual world. In the condition of realizing users anomaly behavior persuasion should be applied rather than force. This will enable organization to keep track of weaknesses of the new paths and stuffs which are insecure practices. When insecure practices are found settings could be change to help solve risk of users to hacktivism. The next chapter employs and discusses fear as a tool which may restrict users' adventurism in the internet and might save many from being victims of hack or path to attacking an organization. However, the challenge is that human mind can easily forget his fear being a victim and fall prey to hacking. Therefore organizations should always make a responsibility to minimize the risk of users. To do this, organizations must have the determinations and the commitment to interact with users.

Chapter eight further relates that hackers are often determined and committed to their course and even provide a very good communication when in group. Thus, there is the need for organization to provide a platform for dissemination of information to enhance communication since ignorance is also a major threat to security.

Out of this challenge followed the chapter nine which implore that hacking today should be viewed as a game which can be won at the same time lost. The most important thing is to understand and accept the possibility of a hack from hacktivists. The authors, however, provided measures which could help to ameliorate the risk from Advanced Persistent Threat

(APT) from hacktivists. Equally important is the manner in which abnormalities are supposed to be detected in chapter 10 through observation, identification and analysis of data patterns to avoid hacking let alone risk the businesses of the organization. As done in the previous chapters, recommendations to face some of these complex cyber security challenges are well highlighted. (P, 62).

In chapter eleven, the authors explain the importance of setting up a response team to practice different possibility tactics and make efforts to tackle both past and new problems as a preparatory ground work to self-defense. Hackers are said to be fast lesson learners which demand equal measure of response to avoid repeating past mistakes. To be able to complete this task easily more experience needed to be shared among groups of different organizations, states and communities. However, security experts find it problematic in sharing experiences with each other since there is no trust among them. Chapter twelve briefly highlights encryptions as hidden weapon despite the fact that there still "computing power, computing parallel and new computing paradigm" (p, 67) which still threatens them in the virtual world. The competition to encrypt is parallel to arms race where parties employ to outwit the system. No matter the complexity of encryption it cannot be said to be hundred percent safe.

Thus, the final chapters 13 and 14 advocated for two things. First, the need to realize the importance of personal responsibility, by changing out attitude toward the use of the internet. Second, making cyber security the central theme in various organizations and the international community. These fundamental two issues are sure way to staying ahead away from hack risk in an attempt to win the cyber security crisis looming in the foreseeable future.

From the above discussion, it is patent that the book despite its brevity still provides a great insight into future of cyber world. Although much of the discussion was centered on business organization not much of cyber security and state role in the international system is discussed. In fact sates issues which mentioned were specific, general sketches and scattered international incident. However, the nature of conflict among organizations, lack of regulations governing the administration of the internet virtual world if extended into the domain of international politics will produce more chaotic hostility if not the same. As a result, it is palpable to conclude the book is more of handbook to understanding cybersecurity.