The Importance of a Postgraduate Degree in Cyber Security

I have decided to embark on a long journey of changing and advancing my competencies in IT infrastructure towards cyber security with an aim of understanding risk, knowing secure IT systems, formulating risk assessment and security policies. As a student of MSc in Cyber Security I hope to leverage my operation experience in IT infrastructure, while learning and developing my cyber security skillset. Wide spectrum of fields one could pursue within the field of cyber security - network security, risk appetites, risk management, malware and intrusion detection, digital forensics, human psychology, compliance and governance - is something that I find very appealing with crucial common denominators such as technology, fast-paced, people and problem solving.

Over the past decade there has been a constant rise in cyber threats across the globe. Despite efforts from organizations through regulations and preventive measures, the complexity of cyber threats have also evolved, underlining severity of cyber-attacks on society at economic and social level.

Moreover, in an era of digitalization to create differential and exclusive competitive advantage in business world has also moved “risk management thinking” to go beyond traditional risks to have robust measures to safeguard our dependency on digitized solutions and perceiving their vulnerabilities regards to integrity, confidentiality and accessibility.

Almost overnight changes to facilitate physical distancing underpinned by COVID-19 pandemic not only have embarked digitalization through home schooling, telecommuting, online meetings, cloud platforms but also have strengthened reliance on digitized solutions. However, such new routines have constantly attracted cyber-hackers to exploit

current events, developments to their own advantage, changing the IT risk landscape as regards to the type of potential exploits and attacks used by the hackers.

For an example, Denmark being ranked at top three as most digital country in the European Union (European Union, 2017; European Union, 2020), in their threat assessment 2020 conducted by the center for cyber security concludes that cybercrime and cyber espionage pose high economic and political threat to Denmark and will continue to remain serious with continued digitalization and dependence on digital services. This was well experienced by the country in early outbreak of COVID 19 pandemic, where authorities and businesses became increasingly vulnerable due to the change in routines and availability of secure systems to facilitate telecommuting (Center for Cyber Security, 2020).

Potential impact of cyber-attacks to some businesses would be risk of losing credibility and brand reputation in their market, while some are more prone to risks related to unreliable data, stolen intellectual property, financial losses due to digital fraud or failure of key operational IT systems.

Certainly, business risks are determined by the nature of the operation, yet understanding the importance of business-critical assets and the impact a cyber-attack could have on these assets, is vital for defining the risk appetite in of the business, while identifying all the risks that a business may be exposed to. Understanding the risk areas help to prioritize cyber security actions underlining preventive, detective, recovery measures. On the other hand, considering holistic approach to cyber risk, it is also vital to assess the vulnerabilities of controls and process, lack of governance as well as human psychology and behaviors.

While an average cost of a record being compromised U$141 to average yearly cost of cyber security breaches approximately U$11 million, cyber security in strictly financial terms is seen as absolute necessity cost (Debar, 2019). Growing cost of cyber attacks also create an environment to have an open outlook on what is happening and to be innovative in terms of network monitoring and better data management techniques. Regards to data management, increasing regularity activities such as General Data Protection Regulation (GDPR) by the European Union, Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), and California Consumer Privacy Act, change focus of businesses to understand what data they have, the source of data, ownership of them and what can be done with them, rather than merely securing the data. A sinister narrative of use of Facebook user data by Cambridge Analytica is just one example of vulnerabilities as well as possibilities that cyberspace and the security measures around that had created.

Conversely, renown global IT advisory firm KPMG with deep market insights, in their Global CEO Outlook study covering 1,261 CEO interviews within 10 key markets (KPMG, 2017) highlights that: '71% of global CEOs see investments in cyber security as an opportunity to find new revenue and innovate, rather than an overhead cost'. Clearly such studies have also laid bare importance of cyber security advances in the technology risk landscape and changes to its use beyond what we can conceive merely as an overhead.

In conclusion, while digitalization offers exponentially augmenting opportunities for new capabilities and initiatives, it is also critical for businesses to manage the risks that are introduced into the cyber environment with growing number high-profile cyber security incidents. One of the most critical success factors to win this battel is to understand both

risk landscape as well as unfolding opportunities around cyberspace, while developing conscious effort to advance cyber security capabilities.

Reference List

Center for Cyber Security. (2020) *The cyber threat against Denmark*. Available from: https://fe-ddis.dk/CFCS/publikationer/Documents/The-cyber-threat-against-Denmark-2020.pdf [Accessed 11 September 2020].

Boehm, J. et al. (2018) *Cyber risk measurement and the holistic cybersecurity approach.* Available from: https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/Cyber%20risk%20measurement%20and%20the%20holistic%20cybersecurity%20approach/Cyber-risk-measurement-and-the-holistic-cybersecurity-approach-vf.pdf [Accessed 15 September 2020]

Debar, H. (February 3, 2019) Cybersecurity: high costs for companies. *The conversation*. Available from: https://theconversation.com/cybersecurity-high-costs-for-companies-110807 [Accessed 15 September 2020].

Deloitte. (2015) *Responding to cyber threats in the new reality - A shift in paradigm is vital*. Available from: https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-thought-leadership-noexp.pdf [Accessed 13 September 2020].

Deloitte. (2018) *Managing Risk in Digital Transformation*. Available from: https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-managing-risk-in-digital-transformation-1-noexp.pdf [Accessed 14 September 2020].

European Commission. (2020) *The Digital Economy and Society Index (DESI) 2020*. Available from: https://ec.europa.eu/digital-single-market/en/desi [Accessed 14 September 2020].

European Commission. (2017) *The Digital Economy and Society Index (DESI) 2017*. Available from: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_17_352 [Accessed 10 September 2020].

European Court of Auditors. (2019) *Challenges to effective EU cybersecurity policy.* Available from: https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf [Accessed 11 September 2020].

KPMG. (2017) *KPMG P/S Annual Report*. Available from: https://assets.kpmg/content/dam/kpmg/dk/pdf/DK-2018/01/KPMG_Denmark_Annual_Report_2017_WEB_version.pdf [Accessed 13 September 2020].

Moreolo, C. (May, 2018)Cybersecurity: Threat or opportunity?. *IPE magazine*. Available from: https://www.ipe.com/cybersecurity-threat-or-opportunity/10024445.article [Accessed 15 September 2020].