The Educational Review, USA, 2017, 2(1), 136-146
http://www.hillpublisher.com/journals/er

Cybersecurity Workforce Development for Digital Economy

Chooi Shi Teoh, Ahmad Kamil Mahmood

Faculty of Science and Information Technology, Universiti Teknologi Petronas, Malaysia

How to cite this paper: Teoh, C. S., & Mahmood, A. K. (2017). Cybersecurity Workforce Development for Digital Economy. *The Educational Reviewing, USA,2(1),* 136-146.
http://dx.doi.org/10.26855/er.2018.01.003

Corresponding author: Chooi Shi Teoh, Faculty of Science and Information Technology, Universiti Teknologi Petronas, Malaysia.

Abstract

The digital economy has revolutionized the global economy by creating the world without borders. It permeates the economic landscape that not only affecting the skill set needed to get a good job but also the surge of advancement and sophistication of cyber threats contributing to the rising demand of skills and expertise in cybersecurity workforce. This paper focuses on the efforts to develop cybersecurity workforce by nations with an objective to examine the National Cyber Security Strategies (NCSS) of nine top ranking nations in digital economy addressing the gap in cybersecurity workforce. From extensive literature review conducted, it was found that the common emphasis of the NCSS are critical in the area of infrastructure protection, cybercrime protection, cybersecurity workforce development, cybersecurity public awareness, research and development (R&D) and international collaborations. Furthermore, there is emerging trend of National Cybersecurity Centers which serves national nexus to preempt, response and mitigate cyber threats and incidents. As cyber threats grow, the demand for cybersecurity workforce reached critical level of shortage expected to be at 3.5 million by 2021. To address this alarming demand, cybersecurity workforce development need to have a long-term effort to satisfy the workforce shortage of today, and also effort to groom and prepare the young ones in school to be interested and serious about getting into cybersecurity industry.

Keywords

Cybersecurity, Workforce Development, Digital Economy, User Awareness, Training

1. Introduction

With internet, Alibaba is capable of achieving USD 25.3 billion sales in a single day, on Single's Day 2017 (Hsu, 2017). The world is in the midst of major global shift as over 3.8 billions of global population are connected online and this number will hit 6 billion by 2022 (Morgan, 2017). The connected world brings unprecedented breakthroughs and opportunities. The internet becomes the means towards economic prosperity and the platform to stir the social change (Cybersecurity, 2016). To be relevant, businesses need to be online and innovate to be part of digital economy. It is business unusual as technology and economy merged to transform the way of doing business to access new market and wealth creation. Information is an agent of integration and enabler of innovation in business (Hemmatfar, Salehi, & Bayat, 2010). The social transformation is happening now as connected world changes our societal fabric in politic, economy, technology and culture. This digital evolution impacts the world in multiple facets, from e-economy, social movements, government elections and awareness of global issues swiftly (Chakravorti, 2016). At the same time, the reliance on cyberspace had generated a trend of rising cyber dependency that it leads to global risks (WEF, 2017).

Digital economy stretches its boundary as technological changes swiftly. One of the most disruptive innovation is bitcoin, which breaks barriers and create new rules. Based on peer to peer agreement, this open network banking becomes the world's first digital currency. The digital currency redefines financial sector, as it removes the middle man, and creates a community to maintain and thrive within the system. In 2010, the first bitcoin transaction for a pizza costs 10,000 bitcoin transacted for a pizza, with each bitcoin at USD 0.0025 (Lee, 2014). On 7th Dec, 2017, bitcoin surpassed USD 16,000, achieving an all-time high (Mullen & Wattles, 2017). The year 2017 sees the meteoric rise of bitcoins which is deemed unsustainable and volatile (Mullen & Wattles, 2017; Rees, 2017). A year ago, it was below USD 800 (Mullen & Wattles, 2017). On the other hand, blockchain and distributed ledger are identified as emerging technologies which exacerbate economic global risks (WEF, 2017). Bitcoins are marred by linkages with Silk Road bust and anonymities of cyber criminals. In 2017, the waves of WannaCry and Petra ransomwares hit globally and demanded payment in bitcoins (Symantec, 2017). The cryptocurrency and blockchain technology will expand and gain prominence as Digital Asset Research Lab was launched as research and development initiative between Blockchain (a software platform digital assets) and Imperial College London's Centre of Cryptocurrency Research and Engineering (IC3RE) (Campbell, 2017).

According to World Economic Forum, the trend of increasing cyber dependency of the population had raised the likelihood of cyberattacks in the global risks landscape 2017 (WEF, 2017). Dependency of every nation on internet connectivity is undeniable, especially in the era of efficiency and efficacy. As digital economy shapes the global economy, secured cyberspace is non-negotiable. With increase dominance and dependence on cyberspace, cyber threats aspect is inescapable in digital progress (Chakravorti, 2016; Hathaway, 2013). The increase in cybersecurity demand had created a global cybersecurity workforce gap. By 2022, the gap in global cybersecurity workforce is staggering 1.8 million (ISC2, 2017). Other resource predicted this number to be higher than expected and to reach 3.5 million workforce shortages in cybersecurity by 2021(Morgan, 2017). The key point is that there is a great shortage and gap between demand and supply of cybersecurity workforce today and the future.

In this article, we focus on efforts to develop cybersecurity workforce by the nations. The objective of this paper is to examine the NCSS of the nine top ranking nations in digital economy and address the gap in cybersecurity workforce in the nations. Cybersecurity is no longer about preventing attack, it is the cornerstone of digital economy (Mulligan, 2017). The rise of advancement and sophistication of cyber threats are contributing to the rising demand and broadening scope of skills of the cybersecurity workforce.

2. Related Work

2.1. Cybersecurity Workforce

Cybercrime is a growing industry which rose to USD 450 billion in 2016 (McAfee, 2014). Other records reported global cybercrime cost to reached USD 575 billion annually (Symantec, 2016). For the top four largest economies (US, China, Japan and Germany), total loss in cybercrime reached USD 200 billion (McAfee, 2014). In cybercrime, the loss not limited to actual losses due to the attack, as it involves recovery and opportunity costs. A study in Italy reported that losses in cybercrime was USD 875 million, yet the cost of recovery and opportunity lost was USD 8.5 billion (McAfee, 2014). However, there is contradictory research results, which debate that the cost of incidents is approximately equal to its annual IT security investment (Romanosky, 2016). In the research, the costs are differentiated as first and third party losses (Romanosky, 2016). Cybercrime also affects company reputation, goodwill and stock prices. Year 2013 is the beginning of cybercrime-driven mega data breaches, with eight mega breaches (Symantec, 2014). A mega breach is defined as a breach of more than 10 million records (Symantec, 2016). In 2015, the trend of mega breaches grew to loss of 429 million identities in mega breaches and yet this number hides a bigger number that remained unreported (Symantec,

2016). The number increased to 1.1 billion total number of identities exposed in 2016 (Symantec, 2017). The year 2016 also has 15 mega breaches, here more than 10 million identities exposed each time (Symantec, 2017).

In the digital world, where both defender and attackers engaged in online battle, skills and knowledge determine the success on the battlefield. It is increasingly difficult to fill the need of cybersecurity workforce. The industry is finding difficulty in finding skilled resources and even hired talents require time and training to be fully up to speed. The attacks are increasing in more hostile environment online, and so is the demand for cyber security professionals. Although growing, the growth rate of cyber security workforce has slowed down (ISACA, 2017). Another main challenge in developing cybersecurity workforce is the length of maturity time needed for cybersecurity professional (Assante & Tobey, 2011). In order to reach the peak performance requires years of IT knowledge packaged with year of security experiences (Assante & Tobey, 2011). In addition, the technology evolves and dynamic, making it an uphill battle in cybersecurity workforce. The online battle field with the advanced cyber threats, can only be managed with skilled cybersecurity workforce with the assistance of cyber-aware users (Assante & Tobey, 2011).

An integrated cybersecurity workforce includes technical and nontechnical positions which are fulfilled with knowledge and experienced talents (Newhouse, Keith, Scribner, & Witte, 2017). In building cybersecurity workforce, three distinguish elements of demand, need and supply important. Demand is defined as the capabilities required in the job description, according to the number of positions available and based on the salary to match the capabilities (Council, 2013). The term need refers to the number of personnel and capabilities required to provide the satisfactory cybersecurity level (Council, 2013). In many cases, demand and need are not equal. If nation or organisation invest less in cybersecurity level, demand is lower than the need. Demand could also be lower if the nation or organisation underestimates the cyber threats (Council, 2013). Supply is the number of qualified workforce to fill the positions. Supply also represents the attractiveness of the cybersecurity work, the availability of the necessary training and education and overall professional market in cybersecurity (Council, 2013). Of the three elements, supply is the most critical one, as the industry is a gap of 1.8 million cybersecurity personnel in 2022.

The glaring threats of cyber attacks to the nations had raised many red flags. To combat and defend the cyberspace, nations identified the pressing need for a strong cybersecurity workforce. The lack of cybersecurity expertise and the widening gap between demand and supply call for urgent actions at the national level (Fourie et al., 2014). In US, National Initiative for Cybersecurity Education (NICE) was created as national initiative to create operational and sustainable cybersecurity workforce (Paulsen, McDuffle, Newhouse, & Toth, 2012). From the initiative, NICE has four components in Cybersecurity Workforce Framework, namely awareness, formal education, training and professional development and workforce structure. In order to achieve well-developed workforce, a research presented Ground Truth Expertise Development cycle (Assante & Tobey, 2011).

2.2. National Cyber Security Strategies in Digital Economy

Opportunities are coupled with risks in this digital evolution. Hyper connectivity exposed nations to cyber threats and brings in the opportunities and abundance potential to boost economy (Teoh & Mahmood, 2017). Digital economy raises the issues of security, privacy and trust (Al-Khouri, 2012). Nations and governments need to employ new technologies to capture the benefits and to improve cybersecurity to mitigate cyber risks. Cybersecurity is key enabler for digital-enabled economy and society. According to a research by Al-Khouri, digital economy refers to economy base on electronics goods and services and formed by electronic business models, integrated with global network of economy and social, enabled by ICT such as internet technologies (Al-Khouri, 2012).

The growth and potential of digital economy depend on the trust on the internet and in cyberspace. 2017 recorded the highest sales on Alibaba's Single's Day with a record of passing USD 1 billion within the first two minutes and USD 25.3 billion for the day (Hsu, 2017). Digital economy is not fully utilised and exploited, and yet it is estimated at 22.5% of the world economy (Knickrehm, Berthon, & Daugherty, 2016). Digital investments have growth multiplier effect in national GDP, where it increases the national economic output. In US, this digital investment is expected to translate into additional 2.1% of GDP in 2020, equivalent to additional USD 421 billion (Knickrehm et al., 2016).

Table 1. National Cyber Security Strategies.

Nations	SGP	FIN	NOR	USA	NLD	CHE	GBR	LUX	JPN
Year	2016	2013	2012	2003	2013	2012	2016	2015	2015
NCSS	CYBER SECURITY STRATEGY	FINLAND'S CYBER SECURITY STRATEGY	CYBER SECURITY STRATEGY FOR NORWAY	NATIONAL STRATEGY TO SECURE CYBER SPACE	NATIONAL CYBER SECURITY 2: FROM AWARENESS TO CAPABILITY	NATIONAL STRATEGY FOR THE PROTECT-ION OF THE SWITZER LAND AGAINST CYBER RISKS	NATIONAL CYBER SECURITY STRATEGY 2016-2021	NATIONAL CYBER SECURITY II	CYBER SECURITY STRATEGY
First NCSS	Yes	Yes	No (2003)	Yes	No (2011)	Yes	No (2009)	No (2011)	No (2006)
Size (pages)	27	44	32	60	36	42	80	41	58
CIP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
CCP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
CWD	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
R&D	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IC	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PA	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IP	No	No	No	No	Yes	Yes	Yes	Yes	No
M	No	No	No	No	No	Yes	Yes	No	No
NCC	2016	2014	2014 (research purpose)	2008	2012	2003 (research purpose)	2016	Planned 2017	2015

Fourth Industrial Revolution has embarked and nations are at infancy transitioning to new era where digital, biological and physical world merge (Schwab, 2016). In this digital revolution, opportunities and growth rest on conducive regulatory and business environment, ICT readiness on emerging technologies, and usage of ICT in societal-wide adoption and leverage (Baller, Dutta, & Lanvin, 2016). For a nation to thrive and prosper in this century, digital intervention is una-

voidable. World Economic Forum published Networked Readiness Index (NRI) to assess and compute nations' readiness to capture and reap the benefits of emerging technologies in digital economy (Baller et al., 2016). The top ten nations based on NRI rankings are Singapore, Finland, Sweden, Norway, USA, Netherlands, Switzerland, UK, Luxembourg and Japan. For this article, Sweden is not included in the analysis as the NCSS is in Swedish.

Articulation and publication of national cyber security strategy (NCSS) is identified as an essential element in order to protect nation ICT investment and enable digital economy, (Hathaway, 2013). To achieve the necessary economic outcome, the NCSS need to state the strategic objectives, identify the responsible and accountable entity, develop specific, measurable, attainable, results-oriented and time-measurable (SMART) outcomes, and commit implementation plan based on available resources and support (Hathaway, 2013).

For nations to capture the opportunities in digital economy, cyber risks and cyber threats are permanent. As nations capitalising on digital revolution, cybersecurity is a national priority to foster economic welfare (Luiijf & Besseling, 2013). From 2013 – 2016, 48 NCSS were released. The main objectives in the NCSS are maintaining secure, resilient and trusted electronic operating environment, promoting economic and social prosperity, promoting trust, business and economic growth, addressing risk of ICT and strengthening resilience of infrastructures (NATO, 2013). As every nation has different priorities and challenges in handling cyber threats, each NCSS has variance in scope and depth. In NCSS, main priorities as roles and responsibilities of cybersecurity, situational awareness, legislation matters, training and R&D, secured ICT products and services and international cooperation (Lehto, 2013). Some of the fundamental elements for NCSS are organisational, legal and technological (Elkhannoubi & Belaissaoui, 2015).

Each of the nine top ranking NRI nations are equipped with NCSS. These NCSS published from 2003 till 2016. It is important that all these strategies remained updated and current, as cyber threat landscape is ever evolving (Norway, 2012). For the purpose of analysis in this article, nine NCSS were analysed as shown in Table 1 (Teoh & Mahmood, 2017). NCSS from Sweden is not included as the document is in Swedish.

The nine NCSS for the nations provided the strategy to build and provide the trusted cyber environment required for digital economy to prosper. In order digital economy to thrive, security is a need (Cybersecurity, 2016). Singapore, Finland and Switzerland owned their first NCSS, published in 2016, 2013 and 2012 respectively. These nations flourish in digital economy due to the strong and effective private sector and industry that support the cyber environment (Teoh & Mahmood, 2017). It leads to increase of digital confidence and trust among the digital citizens and organisations. United States and Norway pioneered the effort of NCSS, with the first NCSS released in 2003. United States had been actively publishing cybersecurity policy and strategy for specific purpose and yet to release another national cybersecurity strategy since 2003(Shafqat & Masood, 2016). Each of the document is purposeful in various aspects of cybersecurity such as cybersecurity workforce framework, critical infrastructure framework and DOD cybersecurity strategy, however it does not synthesise the holistic cybersecurity strategy in US. Japan is pioneer in Asia with the first release in 2006.

From Table 1, the strategic elements in the NCSS are protection of critical infrastructure, defence against cybercrime, cybersecurity workforce development, increasing public awareness, improving research and development (R&D) and international collaborations (Finland, 2013; Luxembourg, 2015; Norway, 2012; Singapore, 2016; Switzerland, 2012; UK.Government, 2016; US, 2015). The element analysed in this article is cybersecurity workforce development.

3. Methodology

This article is based on literature research. The researcher accessed information from variety of literatures, based on journal articles, global reports, current industry happenings and market trends. After the literatures are gathered, the re-

searcher sorts them out to determine the relevance to finalise the representative literature to the topic (Lin, 2009). The relevance of the literatures chosen are based on purpose, authority, effectiveness and reliability (Lin, 2009).

For the purpose of the research, the representative literatures chosen were from year 2000-2017. The issues in cybersecurity are current and fast moving. Representative literature on the topic need to be current to be relevant. In this research, reports, journal article and technology news from reliable sources were included. It provides a review of recent practices and development in cybersecurity workforce and NCSS.

4. Cybersecurity Workforce Development

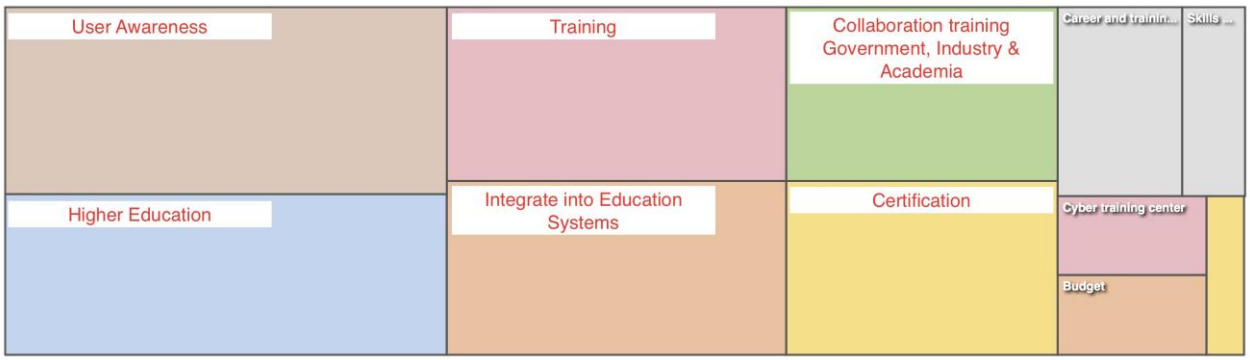

Figure 1. Elements for Cybersecurity Workforce Development.

For the purpose of this article, the focus of analysis is on cybersecurity workforce development and not cybersecurity professional development. The domain of cybersecurity workforce development is larger than professional development. Professional development refers meeting immediate needs of the industry by introducing common bodies of knowledge, principles and guidelines, certifications and trainings (Hoffman, Burley, & Toregas, 2011). On the other hand, workforce development is long-term, with a road map to fulfil the industry need today and generate sustainable pool of talent in the future. The workforce development begins at a younger age, grooming and creating the interest of young generation in the domain of cybersecurity. The NCSS of the nations were analysed in the domain of cybersecurity workforce development. The main elements are as shown in Figure 1.

The main elements for cybersecurity workforce development are user awareness, higher education, training, integration into education system, collaboration training between government, industry and academia and certification. Table 2 shows the elements in accordance to the nations.

User awareness is main element in the cybersecurity workforce development as it is emphasised in each of the NCSS analysed. Cybersecurity is a collective responsibility and requires total effort for each stakeholder in order to strengthen total defence in cyberspace. Everyone should access information about cyber threats, challenges and understand the necessary counter measures. This propel user awareness as the foundation element for cybersecurity workforce development. Every nation has its unique way to promote outreach and awareness activities, some with cooperation and coordination with relevant stakeholders. In Japan, there is a month dedicated for cybersecurity, aptly named "Cybersecurity Awareness Month".

Training is an important element in the development of the workforce. Netherlands has a focus to develop Cyber Defense training and provided the training services through Regional Training Centers. Luxembourg provides training as an avenue for the interested parties to update on the trends of cyber threats and their counter measures. Nation such as USA

is providing the necessary trainings to foster adequate trainings to support the national needs. The training programs provided need to be measured to tabulate its efficiency.

Table 2. Elements for cybersecurity workforce according to nation.

	User Awareness	Higher Education	Training	Integration into Education Systems	Collaboration	Certification
SGP	*	*	*	*	*	*
FIN	*	*			*	*
NOR	*		*			
USA	*	*	*	*		*
NLD	*	*	*	*	*	
CHE	*		*			
GBR	*	*	*	*	*	*
LUX	*	*	*	*	*	
JPN	*		*		*	

Singapore has all the six elements for cybersecurity workforce development. User awareness is prioritised with objective to educate and empower public to be safe in cyberspace. The national strategy to attract and target top talent to grow the cybersecurity workforce. Curricular in higher education tailored to cater and fit cybersecurity industry demand. Scholarships and sponsorship programme are offered to students and to encourage existing cybersecurity talents to deepen their skills. Training and certification are highly encouraged to the current workforce community. Trainings on up-skilling and re-skilling for mid-career professionals also targeted to attract new entrants into the profession. Certification is the avenue to secure and certify the professional skill set based on internationally recognised standards. Collaboration with the industry and academia encourages the transfer of industry need and knowledge into academia, to prepare the students to meet industry expectations. In the NCSS, National Cybersecurity R&D allocated S$190 million in year 2013 trill 2020 for research in aspects of cybersecurity.

Based on UK NCSS, the national strategy for cybersecurity workforce development is complete with user awareness, cybersecurity higher education, training, integration into education system, collaboration between industry, government and academia, certification, allocation of budget, skills advisory, cyber training centre and career and training path. The user awareness effort in UK called Cyber Aware targets to provide advice to public in order to secure them from cyber criminals. In higher education, quality cyber graduate and post graduate education are identified and acknowledged the role of universities in developing and providing skilled talents. UK has long term planning to ensure reliable and consistent cybersecurity workforce. Cyber security education and training are provided to talented 14-18 years old, as to tap the talent at a young age. In addition, cybersecurity and digital skills are part of core courses within the education system. These efforts provide firm foundation for onwards profession into the industry. Certification and accreditation are highly

valued to recognise excellence within the industry and also to provide a focal point to advice, shape and participate in the industry. The UK government has an ongoing effort to provide centre of excellence for cybersecurity training to address specialist skills and wider education. There is also an established fund for retraining personnel to develop their potential and capability in cybersecurity profession. This correlated career and trying pathways in cybersecurity.

In US, the NCSS stated five elements for cybersecurity workforce development, with user awareness, higher education, training, integration with education systems and certification. User awareness covers comprehensive national level awareness program to target businesses, general workforce and the general population to secure the cyberspace. IT security is highlighted as a priority in higher education to foster the young generation into cybersecurity. National Institute of Standards and Technology (NIST) initiative National Initiative for Cybersecurity Education (NICE) engages in awareness, formal education, training and professional development and workforce structure (Paulsen et al., 2012). Under the workforce structure, NICE Cybersecurity Workforce Framework was released (Newhouse et al., 2017). The framework seeks to energise and promote network and ecosystem of cybersecurity education, training and workforce development. NICE Framework assists organisations in terms of workforce identification, tracking and reporting, human capital planning, career progression, qualification requirements, training requirements and standards and standardised development of cybersecurity positions(Newhouse et al., 2017).

Netherlands has a public private partnership (PPP) taskforce to improve the quality and breath of ICT education in all academic level, from primary to professional education. This taskforce is a public private partnership between the industry and the government. The success of the taskforce is to ensure that the skills of the children are honed as early as secondary, in order to ensure the continuity of talent to top degree programs. Personal user awareness is also highly important, as private individuals are tasked and expected to have a certain level of "cyber hygiene". Individuals in Netherlands have personal responsibility to have "cyber hygiene", to ensure the necessary measures to protect themselves in cyberspace are in place.

In Luxembourg, besides user awareness, the authorities focus its effort on ensuring the supply of cybersecurity by training the current workforce and stimulating the interest of the young in computing and programming. For long term, the act of grooming and cultivating the young towards cybersecurity in school involves the students, parents, educators and teachers. At University of Luxembourg, courses and training modules are crafted to meet the demand of the industry and to adopt a response to cybersecurity needs and to build national strength and specificities. To increase the relevancy, public private partnership (PPP) model is used to facilitate training and module development for higher education programs.

In Finland, there is a centre of excellence to spur a robust national cybersecurity cluster. The centre of excellence and the cluster play roles to increase the cybersecurity knowledge and know-how in the nation through education and R&D. Finland also believes in collaboration between government, businesses and non-governmental organisations (NGOs) to develop comprehensive cybersecurity programs to impact the society. In Norway, the authorities provide skills advisory by surveying level of competency of the general public and businesses. Public authorities lead public initiatives to cultivate and sustain the culture of cybersecurity in the nation.

5. Proposal

National level strategy is needed for cybersecurity workforce development. In order to achieve successful development and implementation of this national strategy, below are the proposed steps.

Communication between Different Stakeholders

In order for cybersecurity workforce development strategy to be effective, the stakeholders need to have continuous communications. The government, industry, academia and education system need to be in sync in term of the cybersecurity talent requirements, demands, availabilities and potential. These stakeholders should be included in the development of the cybersecurity workforce national strategy in order to provide inputs and commitments. This will ensure the demand and supply of the talent pool in the nation are in line.

SMART Goals

The national strategy should include SMART (Specific, Measurable, Achievable, Realistic, Timely) goals. Timeline and detailed action plans with defined roles and responsibilities of the stakeholders involved, including the lead agencies. This will increase accountability and commitment of the stakeholders. The success measurement will be a monitoring tool to ensure that the nation in on track towards the cybersecurity workforce goal.

Cybersecurity Workforce Database

The human resource with skills and experience in cybersecurity should be registered in a cybersecurity workforce database. This will provide list of available talent in the nation. It will ease training, mentoring and grooming of cybersecurity workforce. The database can also be utilised as a career path planning and skills advisory. It will avoid loss of cybersecurity talent.

6. Conclusions

The growth of digital dependency of the global population and the explosion of digital economy this year sealed the fact that digital lifestyle and digital economy are here to stay. Digital economy has innovated how the global economy operates and created the world without borders. The Digital Revolution poised new challenges to business and nations, as boundaries are tested and redefined. By 2022, 6 billion global population are expected to connected online (Morgan, 2017). This development is coupled with evolving cyber threats and risks. Cybersecurity is the cornerstone of digital economy now (Mulligan, 2017).

Nations implement National Cyber Security Strategies (NCSS) to address cybersecurity issues and to provide a national level strategic effort to thrive in the cyberspace. The common emphasis of the NCSS analysed are critical infrastructure protection, cybercrime protection, cybersecurity professional development, cybersecurity public awareness, research and development (R&D) and international collaborations (Teoh & Mahmood, 2017). A NCSS should include implementation plan and measurement to enable measurable progress in a timely manner. There is emerging trend of National Cybersecurity Centers which serves national nexus to preempt, response and mitigate cyber threats and incidents. As cyber threats grow, the demand for cybersecurity workforce reached critical level of shortage. The highest number predicted is 3.5 million shortage of cybersecurity workforce by 2021(Morgan, 2017). To address this issue, cybersecurity workforce development is a long-term effort. It involves initiatives to groom and prepare the young ones in school to be interested and serious about getting into cybersecurity industry.

Based on the NCSS analysed, there are six elements of cybersecurity workforce development. The elements are user awareness, training, certification, higher education, collaboration and integration into education systems. Each nation has similar yet unique initiatives to develop their national cybersecurity workforce.

Acknowledgements

This work was supported by International Information Systems Security Certification Consortium Inc $(ISC)^2$ under the Graduate Scholarship.

References

Al-Khouri, A. M. (2012). Emerging Markets and Digital Economy. *International Journal of Innovation in the Digital Economy, 3*(2), 57-69. doi: 10.4018/jide.2012040105

Assante, M. J., & Tobey, D. H. (2011). Enhancing the Cybersecurity Workforce. *IT Professional, 13*(1), 12-15.

Baller, S., Dutta, S., & Lanvin, B. (2016). The Global Information Technology Report 2016: Innovation in the Digital Economy. Geneva: World Economic Forum.

Campbell, R. (2017). Bitcoin Wallet Blockchain Partners Imperial College London to Launch Research Lab [Press release]. Retrieved from https://www.cryptocoinsnews.com/bitcoin-wallet-blockchain-partners-imperial-college-london-launch-research-lab/

Chakravorti, B. (2016). Where the Digital Economy is Moving Fastest. Harvard Business Review: Harvard Business School.

Council, N. R. (2013). Professionalizing the Nation's Cybersecurity Workforce? Criteria for Decision-Making. Washington DC: The National Academic Press.

Cybersecurity, C. o. E. N. (2016). Report on Securing and Growing the Digital Economy. NIST.

Elkhannoubi, H., & Belaissaoui, M. (2015). *Fundamental Pillars for an Effective Cybersecurity Strategy*. Paper Presented at the Computer Systems and Applications (AICCSA).

Finland. (2013). Finland's Cyber Security Strategy: Secretariat of the Security Committee.

Fourie, L., Pang, S., Kingston, T., Hettema, H., Sarrafzadeh, H., & Watters, P. (2014). *The Global Cyber Security Workforce: An Ongoing Human Capital Crisis*. Paper presented at the Global Business and Technology Association Conference.

Hathaway, M. E. (2013). Cyber Readiness Index 1.0. Great Falls, VA: Hathaway Global Strategies LLC.

Hemmatfar, M., Salehi, M., & Bayat, M. (2010). Competitive Advantages and Strategic Information Systems. *International Journal of Business and Management, 5*(7), 158-169.

Hoffman, L. J., Burley, D. L., & Toregas, C. (2011). Holistically Building the Cybersecurity Workforce. *IEEE Security & Privacy, 10*(2), 33-39.

Hsu, T. (2017). Alibaba's Singles Day Sales Hit New Record of $25.3 Billion. *New York Times*. Retrieved from https://www.nytimes.com/2017/11/10/business/alibaba-singles-day.html

ISACA. (2017). State of Cyber Security 2017: Part 2: ISACA.

ISC2. (2017). 2017 Global Information Security Workforce Stduy: ISC2.

Knickrehm, M., Berthon, B., & Daugherty, P. (2016). Digital Disruption: The Growth Multiplier. *Accenture Strategy*.

Lee, T. (2014). Five years of Bitcoin in One Post [Press release]. Retrieved from https://www.washingtonpost.com/news/the-switch/wp/2014/01/03/five-years-of-bitcoin-in-one-post/?utm_term=.5dae8e6c1465

Lehto, M. (2013). *The Ways, Means and Ends in Cyber Security Strategies*. Paper presented at the 12th European Conference on Information Warfare and Security, Finland.

Lin, G. (2009). Higher Education Research Methodology- LIterature Method. *INternational Education Studies, 2*(4), 179-181.

Luiijf, E., & Besseling, K. (2013). Nineteen National Cyber Security Strategies. *International Journal of Critical Infrastructure, 9*.

Luxembourg. (2015). National Cybersecurity Strategy II. 23.

McAfee. (2014). Net losses: Estimating the Global Cost of Cybercrime.

Morgan, S. (2017). Top 5 Cybersecurity Facts, Figures and Statistics for 2017. *CSO*.

Mullen, J., & Wattles, J. (2017). Bitcoin Was $800 a Year Ago. Now It's $16,000. *CNN*. Retrieved from http://money.cnn.com/2017/12/06/investing/bitcoin-rally-hits-14000/index.html

Mulligan, C. (2017). Cybersecurity: Cornerstone of the Digital Economy. *Imperial College Business School London*.

NATO. (2013). National Cyber Security Strategy Guidelines. Tallinn, Estonia.

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework: NIST.

Norway. (2012). Cyber Security Strategy for Norway. 32.

Paulsen, C., McDuffle, E., Newhouse, W., & Toth, P. (2012). NICE: Creating a Cybersecurity Workforce and Aware Public. *IEEE Security & Privacy, 10*(3), 76-79.

Rees, T. (2017). Bitcoin Touches over $16,000 but Most Institutional Investors Believe Iit Is an Unsustainable Bubble. *The Telegraph*. Retrieved from http://www.telegraph.co.uk/business/2017/12/07/bitcoin-soars-towards-15000-ladbrokes-coral-shares-jump-gvc/

Romanosky, S. (2016). Examining the Costs and Causes of Cyber Incidents. *Journal of Cybersecurity*, tyw001. doi: 10.1093/cybsec/tyw001

Schwab, K. (2016). Fourth Industrial Revolution

Shafqat, N., & Masood, A. (2016). Comparative Analysis of Various National Cyber Security Strategies. *International Journal of Computer Science and Information Security*, *14*(1), 129-146.

Singapore. (2016). Singapore's Cybersecurity Strategy. 27.

Switzerland. (2012). National Strategy for the Protection of Switzerland against Cyber Risks. 42.

Symantec. (2014). 2014 Internet Security Threat Report.

Symantec. (2016). 2016 Internet Security Threat Report (Vol. 21).

Symantec. (2017). 2017 Internet Security Threat Report (Vol. 22).

Teoh, C. S., & Mahmood, A. K. (2017). *National Cyber Security Strategies for Digital Economy.* Paper presented at the Research and Innovation in Information Systems(ICRIIS).

UK.Government. (2016). National Cyber Security Strategy 2016-2021.

US, D. (2015). The Department of Defense Cyber Strategy.
WEF, W. E. F.-. (2017). The Global Risks Report 2017. Geneva: World Economic Forum.