مبادرات محمد بن راشد آل مكتوم العالمية
Mohammed Bin Rashid
Al Maktoum Global Initiatives

كلية محمد بن راشد للإدارة الحكومية
MOHAMMED BIN RASHID
SCHOOL OF GOVERNMENT

Policy Analysis Exercise No 011

May 2022

MOHAMMED BIN RASHID SCHOOL OF GOVERNMENT

POLICY ANALYSIS EXERCISE

Summary

This brief looks into ways to enhance the UAE cyber security practices and provide policy recommendations to the relevant stakeholders. The current cyber gaps were found to include outdated software, relative lack of awareness about cyber threats among the general population, and lack of capacities. A benchmarking exercise with countries that possess advanced experience in this domain, such as Australia, Estonia, and Singapore, was conducted to explore successful practices that can help close these gaps. These practices were used as activities and drivers in the Theory of Change to help achieve the desired impact which is the prevention or minimizing of cyber-attacks and curbing economic losses. The findings point to several policy measures and regulations that can be deployed to advance cybersecurity practices in the UAE. These include updating and patching the current software systems; authorizing professional white-hat hackers to take part in bug bounty programs across the country, and using their know-how to upskill and train UAE specialists and cadres. Furthermore, inter-society campaigns and programs are needed to raise awareness, including induction training at the workplace and digital citizenship classes in school curricula.

Author: Fatima Ali
Supervised By: Dr. Saeed Aldhaheri

Advancing Cybersecurity in the UAE

UAE Cybersecurity Progress

Cybersecurity is a multi-faceted domain; the Merriam–Webster dictionary defines cybersecurity as “measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack”[1]. In the government context, this could be interpreted as the measures and interventions that government entities take to protect institutions and the public against threats in cyberspace such as cybercrime, espionage, cyberterrorism, cyberwars, etc.. Meanwhile, ransomware and malware, such as Flame and Shamoon, have been increasingly spreading, posing a threat to both home and corporate users. Thus, cybersecurity covers both, personal and institutional use. On the individual’s level it is referred to as protection against viruses and malware whether at home or in the workplace, which makes cybersecurity a shared responsibility. Cybercriminals often target and operate in countries with weak cybersecurity measures and they often choose communities that lack awareness about this subject.

About the PAE Series

The Policy Analysis Exercise (PAE) series is a student-led policy publication series. The PAE Series is a platform that highlights the contribution of MBRSG postgraduate students to policy. The Policy Briefs in this series identify and analyze real policy issues and provide concise advice and solutions for policymakers. The Series contributes to bridging the gap between educational output and real policymaking. It highlights the impact of MBRSG’s educational output on policy through high quality research outcomes by MBRSG students. For policymakers, the Series provides valuable practice-driven policy analysis, advice, recommendations and solutions that can contribute to better quality of government.

The UAE strategy landscape that governs digital technologies as shown in Figure 1 consists of individual integrated national strategies that complement each other and act as enablers to serve long-term visions such as the UAE Vision 2071. No wonder that the National Cyber Security stands among these top strategies. The growing importance of cybersecurity is evident by the size of its market, which is estimated at AED 1.8 billion in the UAE alone, and AED 18 billion in the Middle East and North Africa (MENA). Driven by particularly strong growth in the GCC, the MENA cybersecurity markets are expected to be worth more than AED 36 billion by the end of 2022[2].

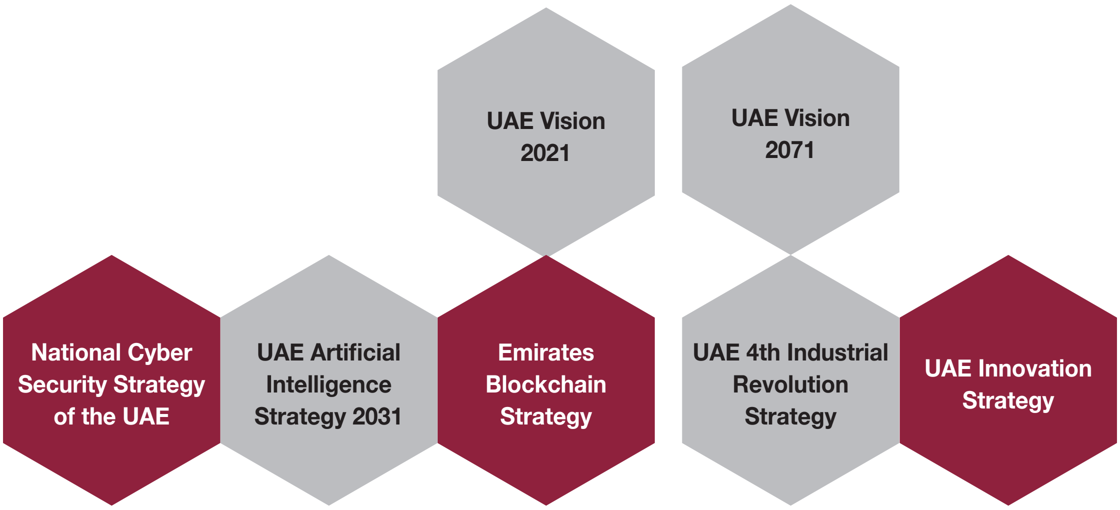
UAE Vision 2021
UAE Vision 2071
National Cyber Security Strategy of the UAE
UAE Artificial Intelligence Strategy 2031
Emirates Blockchain Strategy
UAE 4th Industrial Revolution Strategy
UAE Innovation Strategy

Figure 1. The UAE strategy landscape Source: (Author)

Through its Cybersecurity Strategy as shown in Figure 2, the UAE aspires to enable citizens to securely participate in the digital world, foster a culture of entrepreneurship in cybersecurity, allow

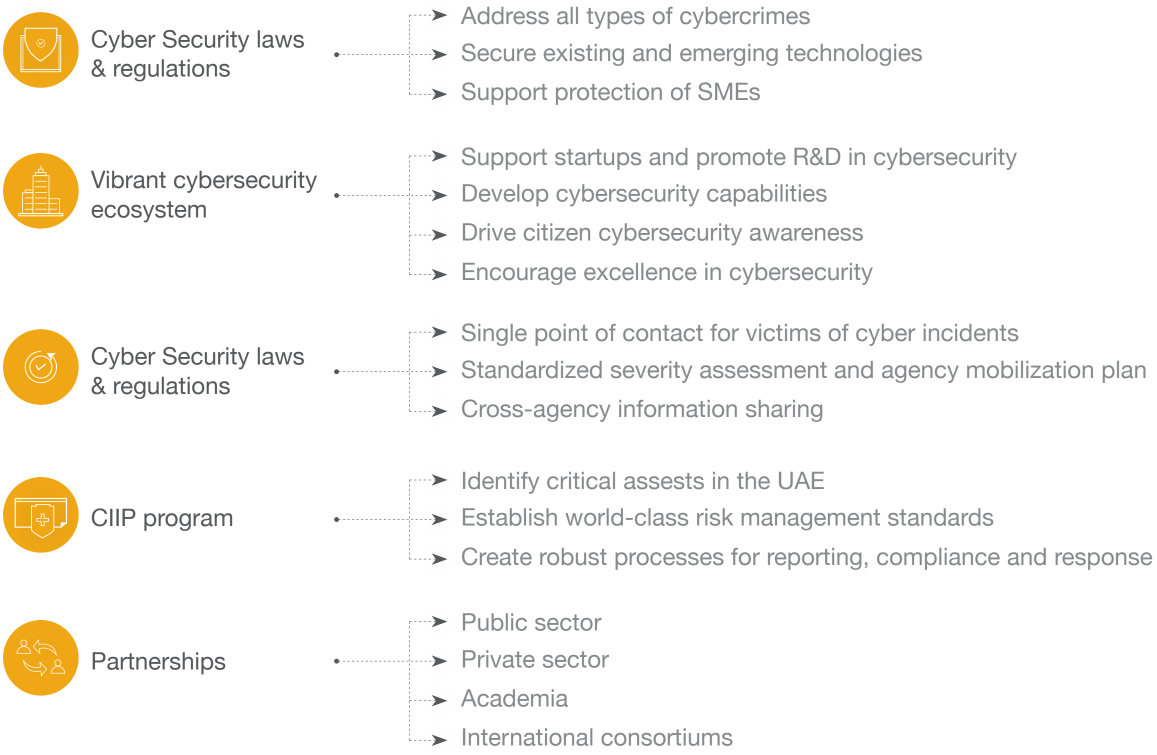
Cyber Security laws & regulations
Address all types of cybercrimes
Secure existing and emerging technologies
Support protection of SMEs
Vibrant cybersecurity ecosystem
Support startups and promote R&D in cybersecurity
Develop cybersecurity capabilities
Drive citizen cybersecurity awareness
Encourage excellence in cybersecurity
Cyber Security laws & regulations
Single point of contact for victims of cyber incidents
Standardized severity assessment and agency mobilization plan
Cross-agency information sharing
CIIP program
Identify critical assests in the UAE
Establish world-class risk management standards
Create robust processes for reporting, compliance and response
Partnerships
Public sector
Private sector
Academia
International consortiums

Figure 2. UAE Cybersecurity Strategy – Source: https://u.ae

SMEs to safeguard themselves against cyber-attacks, protect critical information infrastructure assets and build a world-class cybersecurity workforce in the country. The strategy is based on 55 pillars and 60 initiatives to mobilize the collective cybersecurity ecosystem nationally.

In the last five years the UAE has started taking forward steps to build a strong cybersecurity environment with cybersecurity strategies, laws, and initiatives through collaboration between government, academia and the private sector, and building international partnerships. Some of these initiatives are listed in table 1.

Year	Instrument	Type	Issuer
2012	Federal Law No.5 of 2012 on Combatting Cybercrimes and its amendment by Federal Law No.12 of 2016	Law	Federal
2015	Emirates Safer Internet Society (eSafe Society)	Initiative	Non-profit, civic-society
2017	Dubai Cyber Security Strategy	Strategy	Dubai Government
2019	Telecommunications Regulatory Authority (TRA) launched the UAE's Cybersecurity Strategy	Strategy	Federal
2019	Federal Law on Information and Communication Technology in the Health Field of 2019 (the Health Data Law)	Law	Federal
2019	The new Internet of Things (IoT) regulatory framework	Policy and procedure	Federal
2019	Dubai Cyber Think Tank	Initiative	Dubai Government
2019	Mohammed Bin Zayed University of Artificial Intelligence	Initiative	Abu Dhabi Government
2020	UAE appointed its first Chief of Cyber Security	New office	Federal
2020	UAE Cybersecurity Council was established	Council	Federal
2020	Dubai Cyber Index	Index	Dubai Government
2020	UAE Council for Digital Wellbeing	Council and portal	Federal
2020	Aqdar Cyber Awareness	Initiative	Federal
2020	UAE Promise Guidelines	Charter	Federal
2021	UAE Data Protection Law	Law	Federal

Table 1. UAE efforts and initiatives in cybersecurity – Source: (Author)

In the Global Cybersecurity Index (GCI) 2020 published by the International Telecommunication Union (ITU), the UAE jumped 33 places since the last edition of the index, ranking 5th among 193 countries as shown in Table 2, underscoring its efforts to improve cybersecurity practices in the country.

Country Name	Score	Rank
U.S.A.	100	1
United Kingdom	99.54	2
Saudi Arabia	99.54	2
Estonia	99.48	3
South Korea	98.52	4
Singapore	98.52	4
Spain	98.52	4
Russian Federation	98.06	5
United Arab Emirates	98.06	5
Malaysia	98.06	5
Lithuania	97.93	6
Japan	97.82	7
Canada	97.67	8
France	97.6	9

Table 2. UAE ranking in Global Cybersecurity Index Source: ITU - GCI 2020

In recent years, UAE has taken numerous measures to increase its cyber protection capabilities including launching a federal cybersecurity strategy in 2019 and the UAE data protection law in 2021. These initiatives contributed to improving UAE's position in the global digital arena.

Policy Implications

Cybersecurity in the UAE is shaped by global factors, especially the global doubling of cyber-attacks in 2016 and 2017, which resulted in big losses for the global economy estimated at $608 billion (2014-2017) – a cost of $3.2 million on average per a cyber incident[2]. Moreover, cyber-attacks pose real threats to national security and various industries like energy. For example, a cyber-criminal group took a major US fuel pipeline offline in early May 2021 which compromised the pipeline's networks, and led to US fuel prices surging by 6% per gallon[3].

Furthermore, half of the world's population is already online (4.2 billion active internet users worldwide), and they are leaving an ever-growing digital footprint. The UAE also has one the highest social media penetration rates globally with 98.9% of the population active on social media[3]. The UAE has experienced 1.1 million instances of phishing and witnessed a 250% increase in cyberattacks in 2020, mostly phishing and ransomware incidents in addition to other large-scale cyberattacks, especially after the normalization of relations with Israel[4].

According to a 2020 study, the cost of a data breach in Saudi Arabia and the UAE has increased by 9.4 percent throughout the previous year. These instances cost companies $6.53 million per breach on average, which is greater than the global average of $3.86 million per breach. Moreover, such breaches in both countries cost businesses on average $188 per lost or stolen record[5].

The UAE government is well aware of the risks of the so-called 'cyber pandemic' as hackers are taking advantage of Covid-19 related digital adoption to initiate a digital pandemic[6]. However, the field of cybersecurity needs special attention in the UAE for three main reasons or considerations: Firstly, is the level of the country's digitalization and interconnectedness, which includes increased digitalization, outdated software systems and the sophistication and complexity gap. Secondly, the current gap in public awareness, which is generally observed in society and the workplace, and is reflected in policies.

The final consideration is building national capacity to address the shortage in specialists and outsourcing, and upskill and reskill the existing cadres, as highlighted in the UAE cybersecurity gaps table which we have highlighted in Table 3.

1- Systems: The government is making efforts on the federal and local levels to make the UAE a "digital nation", which include initiatives like The UAE Promise, 5G, digital government, among others in the fields of education, economy, human development, and health[7]. However, there is a need to update the outdated software systems with the latest security patches across these sectors (i.e. hospitals, clinics, schools or any institution that requires official documents from clients) in addition to bridging the systems sophistication gap between federal and local governments, as well as public and private establishments.

2- Awareness of types and levels of protection needed for staff of government entities, businesses, society, and individuals: Around 25 percent of people in the UAE admit they do not use any cyber protection, while another 25 percent state they don't take extra precautions to protect their data, devices, and privacy[8]. Effective legislative frameworks need to be coupled with supporting standards and policies to empower and guide against the latest cyber risks and threats, especially in workplaces that do not provide induction programs. This needs to take place across all of the government-defined sectors with priority to protect critical assets, which include energy, electricity and water, government, ICT, finance and insurance, emergency services, health services, transportation, food, and agriculture.

3- Capacity: There is an increased reliance on digitalization in the UAE, therefore an increased need for capacity building in the field. Globally, cybersecurity teams are reactive rather than proactive, and suffer shortages which leads to resourcing[9]. According to the World Economic Forum's Global Cybersecurity survey 2022, there is a 59% shortage of skills in cybersecurity teams which causes challenges when responding to cybersecurity incidents[10]. The upskilling and reskilling should incorporate up-to-date skills, including detecting latest and sophisticated threats, malware analysis and reversing, programming languages, penetration testing, cloud security, and others, especially in the healthcare and banking sectors among other government entities[11].

Gap	Details
Systems	Outdated systems; systems sophistication gap
Lack of awareness	Society; workplaces
Lack of capacity	Specialists' shortage; the need for upskilling and reskilling

Table 3. UAE Cybersecurity gaps Source: Author

The three main issues that need to be addressed in order to enable the advancement of UAE cybersecurity involve the status of the currently used systems, the level of awareness, and the existing cadres of specialists. The outdated systems, the lack of awareness and capabilities will be the gaps addressed by the benchmarking exercise in the next section.

Benchmarking

To protect and promote safety, privacy, responsibility, and cybersecurity as well as to enhance public understanding of the potential impact of cyber-attacks, including social engineering such as phishing, spear phishing, baiting, malware, pretexting, Quid Pro Quo, tailgating, vishing, and water-holing, appropriate policies should be put in place. The policies will educate the public on societal and economic impacts of such threats on personal and professional levels through education curricula and periodic induction programs in workplaces, public lectures, and extending the reach to individuals through popular social media channels. Although cybersecurity in the private sector is still an internal business matter for each company in the UAE, it falls upon the authorities to set a legislative framework capable of keeping pace with innovative technological development while protecting against criminal opportunism for the benefit of the private sector. Effective policies should address the use of up-to-date cybersecurity system software in the workplace, and the organization of workforce training and awareness workshops, in addition to the development of expertise (or even outsourcing in some non-sensitive areas) in the field.

A benchmarking exercise as presented in Table 4 was conducted to explore case studies and ways to help advance the UAE's cybersecurity bridge the gaps identified. The benchmark countries were chosen based on their identification as cases of best practices and for their innovative and holistic attempts to solve similar gaps such as outdated systems, lack of awareness, and lack of capacities. Estonia, which ranked 3rd in e-government adoption in the United Nations e-Government Development Index (2020), was chosen as a benchmark for its X-Road project[12]. As for lack of awareness in cybersecurity, Australia, which ranked 1st in the 2019 Digital Quality of Life index, was selected as a benchmark for its CyberSmart program[13]. Finally, regarding the capacity gap, Singapore was chosen for its innovative solution, particularly the bug-bounty program and white hat hackers.

Gap	Benchmark	Policy option	Impact	Cyber-attacks risk if addressed
Outdated systems	Estonia: X-Road	Update and interconnect the systems in use	Alignment with cybersecurity strategy	Cyber-attacks risks are reduced: updated systems perform better when countering cyber-attacks. At the same time, more digitalization opens up doors for new threats.
Lack of awareness	Australia: CyberSmart and CyberSafetyHelp	Awareness and induction programs in schools and workplaces	Educational	cyber-attacks risks are reduced: raising awareness will increase protection against cyber-attacks and promote healthy digital citizenship.
Lack of capacities	Singapore: White Hackers and bug bounty programs	Training and recruitment	Increase effective use of cybersecurity	cyber-attacks risks are reduced: Deploying advanced technologies and methods to counter cyber-attacks.

Table 4. A benchmark of countries selected to address the current gaps for policy options

A. E-transformation and updating current systems

Estonia is a small country in Northern Europe with a population of 1.3 million. The e-residents can sign up for digital identification cards and signatures to access a wide array of national e-services and databases. Estonia first introduced an electronic identification scheme with digital signatures that gives access to government as well as private sector services in healthcare, banking, and education. Over the years, the list kept growing and now all sectors are connected by a nationwide decentralized databases with a backbone called X-Road[15]. Effectively, 99 percent of Estonia's state services are provided online, with more than 2,600 services that can be used via X-Road[15]. E-Healthcare and Telemedicine are among these services. Estonia Paramedics, for instance, have access via an app using X-Road to all medical records of patients[16]. Estonia is also widely recognized for pioneering in e-governance and e-democracy[17]. These results were achieved by working constantly on the long term across multiple disciplines, and it required agile responses from the government. There was high level of transparency with the system, especially in case of errors, which nurtured the citizens' understanding and acceptance of the system [18].

B. Awareness

UNESCO defines digital citizenship as "a set of skills that enable citizens to access, retrieve, understand, evaluate and use, to create as well as to share information and media in all formats, using several tools, in a critical, ethical and effective way to participate and engage in personal, professional and social activities"[19]. Accordingly, the digital transformation would require preparing citizens to allow them to take advantage of technology to connect with the government online and use the digital services. Also, they should be aware of key concepts such as public information access and data protection rights. They should be able to manage the risks associated with the digital environment and know where to report in case of facing problems. They should also be able to protect themselves and their workplaces from any cyber danger, not to mention their families, considering the great extent of integration of technology in today's society that influences even children's lives.

In the Australian case, the government put in place several programs to educate and enable its citizens to use the internet safely. One major program is the CyberSmart program, which aims to support and encourage children and youth to engage in the digital economy productively while taking the responsibility to protect themselves and others by demonstrating a positive, ethical, and balanced online behavior. The program also targets parents, teachers, and staff. It focuses on four key concepts: digital footprint, digital reputation, digital citizenship, and digital media literacy. It uses various activities, including interactive games, lesson plans, advocacy and educational videos, in addition to teacher training programs, outreach programs, and forums. The program relies heavily on research to develop the proper interventions and material that are evidence-based and user-tested. The research studies produced are shared and linked to cross-government and cross-sector programs to collaborate and organize activities[19]. Complementary programs were also designed and set up in close coordination with public advisory groups, such as the CyberSafetyhelp program, which offers 24-hour services, providing users a safe venue to talk, report, and learn. Australia was ranked at the top of the 2019 Digital Quality of Life index.

C .Capacity building

In 2013, Singapore launched a five-year National Cyber Security plan to secure Singapore's cyber environment. In 2015, the Cyber Security Agency was established to develop a national strategy to tackle cyber threats. The strategy aims to harmonize public and private sector efforts to protect national systems in 10 critical sectors. Additionally, the country has been partnering with like-minded nations to spur international collaboration on this front. In 2018, the Government Technology Agency and Cyber Security Agency announced a partnership with local and international hackers on a Government Bug Bounty program.

Under this program, hackers were invited to search for and uncover vulnerabilities in internet-facing government ICT systems. In return, the hackers were rewarded with monetary prizes ranging from $250 to $10,000 depending on the severity of the bug discovered[20]. Bug bounty programs proved to be economically beneficial, as long as they are not too costly, to entice professional hackers.

There are two benefits from such programs: attack diversion and protection delegation. The former means to divert the hackers away from attacking one's system. The latter means to delegate the protection against-naive hackers to professional hackers[21].

The Theory of Change for enhancing the Cybersecurity practices in the UAE

This section will illustrate the desired advancement in UAE cybersecurity as based on study cases. The theory of change was applied to illustrate how UAE cybersecurity practices could be enhanced based on the best practices established in the benchmarking exercise. The theory of change can be defined as "a method that explains how a given intervention, or set of interventions, is expected to lead to specific development change, drawing on a causal analysis based on available evidence"[22].

The ultimate desired goal, when it comes to cybersecurity, is to prevent cyber-attack and curb economic losses. This will require the allocation of funds, policies, and regulations to support activities (best practices) and achieve the desired outcomes.

The theory of change is a comprehensive mapping to illustrate how and why the desired change is expected to take place in a particular context. It shows how change happens in the short, medium and long term to achieve the envisioned impact.

- It starts with inputs, which are the resources used to develop the intervention. Funding, policy, and regulations are put in place as enablers to kick start the intervention.

- Activities are the actions taken in the mobilization of resources. A number of major tasks, based on the identified gaps and best practices established above, should be completed. Firstly, is the elimination of outdated and legacy systems, and building a national interconnecting system to help strengthen cybersecurity. This can be supplemented by adjusting licensing to ensure systems are updated. Secondly, cybersecurity specialists should be trained and employed, along with the use of hackers in bug bounty programs, to address the capacity gap. Thirdly, introducing induction programs in the workplace, and carrying awareness and educational campaigns will address the awareness gap.

- Outputs are the products from this intervention: increased awareness; inclusion of induction programs in the workplace, digital citizenship in schools; and updating systems are the expected outputs.

- Outcomes are likely to be achieved in the short and medium terms, which may include, for instance, reduced cyber-attacks and having an efficient, interconnected system.

- Impacts are the long-term effect produced by the development of the intervention. Cyber-attack prevention and curbing economic losses are the desired impacts. (Figure 3)

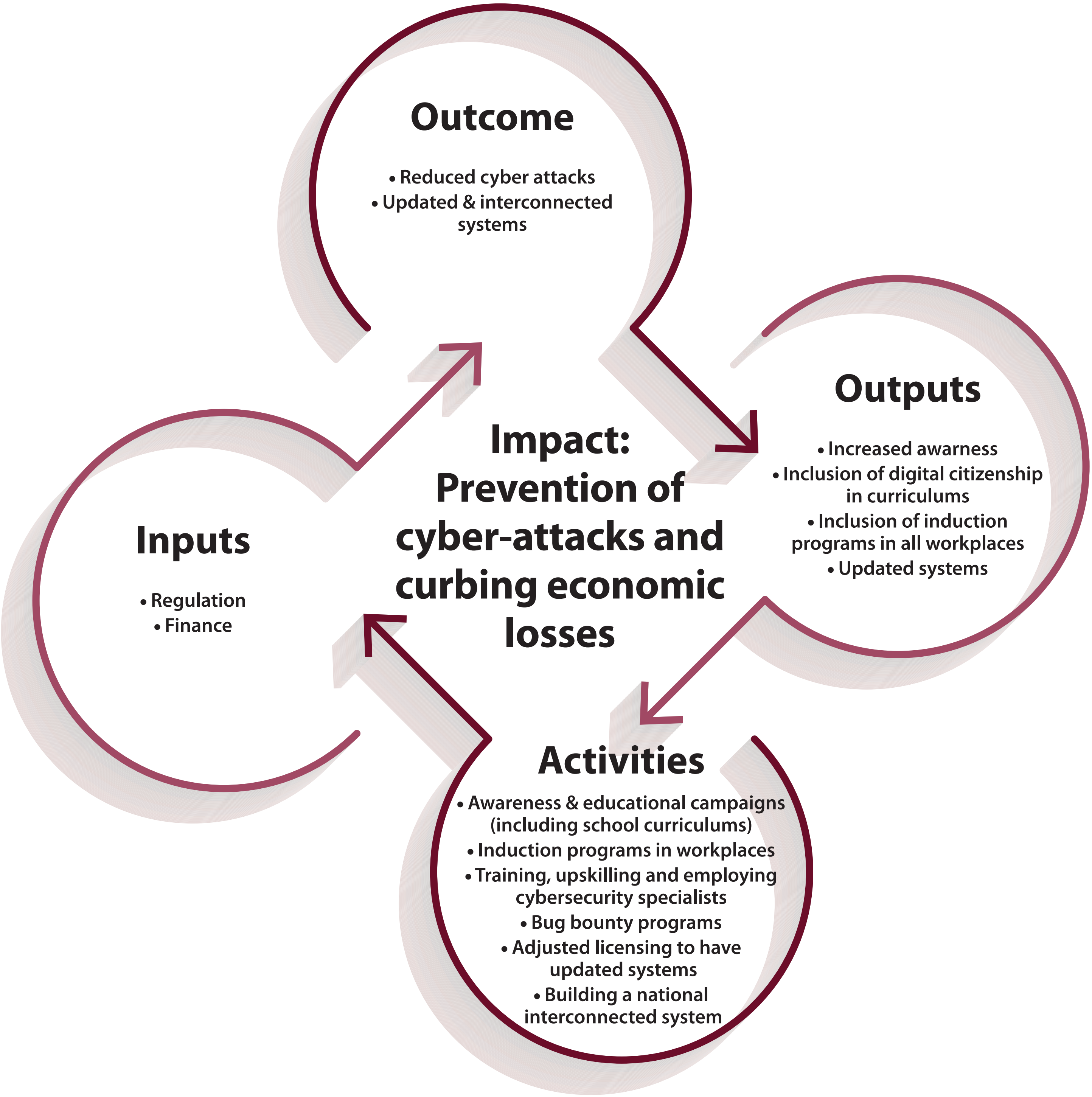
Outcome
• Reduced cyber attacks
• Updated & interconnected systems
Outputs
• Increased awarness
• Inclusion of digital citizenship in curriculums
• Inclusion of induction programs in all workplaces
• Updated systems
Impact: Prevention of cyber-attacks and curbing economic losses
Inputs
• Regulation
• Finance
Activities
• Awareness & educational campaigns (including school curriculums)
• Induction programs in workplaces
• Training, upskilling and employing cybersecurity specialists
• Bug bounty programs
• Adjusted licensing to have updated systems
• Building a national interconnected system

Figure 3. The theory of change for advancing cybersecurity practices in the UAE - Source:Author

Recommendations

- **Government level:** Governments have to be agile and nimble to block and/or limit cybercrimes and cyber threats. The UAE has been very innovative when it comes to cybersecurity, and it constantly introduces new initiatives to tackle all cybersecurity aspects.

The UAE National Cyber-Security office could conduct regular surveys to learn about growth areas to help it focus its efforts where required. Moreover, the UAE Cybersecurity Council could strengthen collaboration with all stakeholders, including civic society, NGOs, and tech companies, to enhance cybersecurity efforts. Launching annual challenges and awards in cybersecurity and bug bounty programs would contribute to achieving this goal.

- **Organizations:** On an organizational level, it is crucial to bridge the digital gap between different entities (private/public, among local governments in UAE, local/federal) by setting policies in place to ensure that their software systems are up-to-date in terms of cybersecurity measures. One way to monitor this is by the authorities in charge of licensing entities and their renewal such as the Ministry of Finance on the federal level, the Departments of Finance on local levels, and the respective local authorities in each emirate such as Abu Dhabi Digital Authority (ADDA) and Dubai Digital Authority (DDA); this will provide a suitable maturity level of digitization.

- **Raising Awareness:** The Ministry of Education, Abu Dhabi Education Department (ADEC), and Knowledge and Human Development Authority (KHDA) could include digital citizenship and awareness in school curricula throughout the education journey.

Additionally, the Ministry of Human Resources and Emiratisation (MOHRE) and the local human resources authorities in Abu Dhabi, Dubai and Sharjah should mandate periodic induction programs about cybersecurity in the workplace, which should be regarded as lifelong education, to capture and counter new trends. This will enable citizens and residents to realize the risks of cyberspace and influence their mindsets to practice cyber hygiene. Special programs for digital illiteracy should also be developed to support senior citizens.

- **Capacity building:** It is vital to up-skill and re-skill current employees in the field of cybersecurity. To a large extent, cybersecurity specialists in the UAE are more reactive than proactive due to skills shortages. Hackers are more agile and sophisticated; they use advanced technologies such as machine learning. The UAE cybersecurity office, along with the respective authorities on the local levels, could authorize hiring white hat hackers or ‘ethical hackers’ to counter malicious hackers. Other measures that can be used are hacking back and security by design. White hat Hackers can also be utilized in educational programs to upskill and reskill current employees in the field.

- **Partnerships:** Cooperation on national level, and forging partnership between the UAE government and other governments to cooperate and exchange intelligence in this field, will help in mitigating threats such as cybercrimes and cyberattacks on critical infrastructure in the future.

Way Forward

Cybercrimes and other illegal online activities cost countries, organizations, and individuals big losses in many ways; whether financial, reputational or psychological. It is essential for governments and businesses to plan cost-effective strategies to curb potential losses caused by cybercrimes.

No doubt, cybersecurity is vital for smart nations. Databases containing vital information, such as medical, financial and other sensitive records, can be misused, breached and exploited . UAE’s implementation of the national cybersecurity strategy and activating the above recommendations could eliminate or reduce many of the risks and threats. The strategy needs to be revised, updated and adjusted by qualified experts to ensure it lives up to all existing and potential challenges. Meanwhile, strong collaboration between all stakeholders on the federal and local levels, as well as users, is vital to try to keep cybersecurity always a couple of steps ahead of threats.

References

1 Merriam-Webster Dictionary (MW). (2020). Cybersecurity. Retrieved from https://www.merriam-webster.com/dictionary/cybersecurity

2 TRA (Telecommunication Regulatory Authority) National Cyber Security Strategy. Available at: https://www.tra.gov.ae/userfiles/assets/Lw3seRUalMd.pdf

3 BBC (2021)'US fuel pipeline hackers 'didn't mean to create problems' Available at: https://www.bbc.com/news/business-57050690

4 Global Media Insight – UAE Social Media Statistics 2020. Available at: https://www.globalmediainsight.com/blog/uae-social-media-statistics/#:~:text=According%20to%20the%20latest%20statistics,annual%20growth%20in%20internet%20users.

5 ITP (2020)'IBM: Cyber breaches cost enterprises in the UAE and KSA over $6.5m per attack in 2020' Available at: https://www.itp.net/news/93473-ibm-cyber-breaches-cost-enterprises-in-the-uae-and-ksa-over-65m-per-attack-in-2020

6 CNBC (2020)'Middle East facing cyber pandemic amid COVID 19 UAE official says' Available at: https://www.cnbc.com/2020/12/06/middle-east-facing-cyber-pandemic-amid-covid-19-uae-official-says.html

7 UAE Promise Guidelines (2020) Available at: The UAE Promise - The Official Portal of the UAE Government

8 Khaleej Times (2021)'Cyberattacks in GCC unlikely to subside in 2021' Available at: https://www.khaleejtimes.com/business/cyberattacks-in-gcc-unlikely-to-subside-in-2021

9 Ramsey, J. (2018) 'Cybersecurity Trends: What to Expect in 2018 and Beyond'. Secureworks. Available at: https://www.secureworks.com/blog/cybersecurity-trends-what-to-expect-in-2018-and-beyond

10 Huxey (2019) 'An overview of the Cyber Security landscape in the UAE' Available at: shorturl.at/jACVY

11 UN E-Govemernent Survey 2020. Available at : UN E-Government Survey 2020

12 UN e-Government Development Index (2020) Available at: E-Government Development Index (EGDI) leaders 2020 | Statista

13 Digital Quality of Life index (2019) Available at: surfshark.com

14 Athens, G. (2015) 'Estonia A Model for e-Government' Society Journal. Vol.58, No.6

15 Government website (e-estonia.com)

16 Heller,N. (2017) ‘Estonia, the Digital Republic’. Available at: https://www.newyorker.com/magazine/2017/12/18/estonia-the-digital-republic

17 Goede, M. (2019) ‘E-Estonia: The e-government cases of Estonia, Singapore, and Curaçao’ Archives of Business Research, 7(2), 216-227.

18 Urabn, M. (2018) ‘Abandoning Silos: Key Takeaways’ Availabe at: https://www.academia.edu/37959844/Abandoning_Silos_Key_Takeaways

19 UNESCO ‘Fostering Digital Citizenship through Safe and Responsible Use of ICT’ Available at: https://en.unesco.org/icted/sites/default/files/2019-04/62_fosteing_digital_citizenship_through_safe_and_responsible_use_of_ict.pdf

20 CIO, ‘Singapore Agencies partner with white hackers to uncover govt systems vulnerabilities’ Available at: https://www.cio.com/article/3329748/singapore-agencies-partner-with-white-hackers-to-uncover-govt-systems-vulnerabilities.html

21 Zhou, J.,Hui,K. (2020) ‘ Sleeping with the Enenmy: An Economic and Security Analysis of Bug Bounty Program. HKUST Business School Research Paper No. 20201-038 Available at: Sleeping with the Enemy: An Economic and Security Analysis of Bug Bounty Programs by Jiali Zhou, Kai-Lung Hui :: SSRN

22 United Nations Development Group, Theory of Change. Available at: Microsoft Word - UNDG-UNDAF-Companion-Pieces-7-Theory-of-Change.docx

About the PAE Series

The Policy Analysis Exercise (PAE) series is a student-led policy publication series. The PAE Series is a platform that highlights the contribution of MBRSG postgraduate students to policy. The Policy Briefs in this series identify and analyze real policy issues and provide concise advice and solutions for policymakers. The Series contributes to bridging the gap between educational output and real policymaking. It highlights the impact of MBRSG's educational output on policy through high quality research outcomes by MBRSG students. For policymakers, the Series provides valuable practice-driven policy analysis, advice, recommendations and solutions that can contribute to better quality of government.

Disclaimer

The views expressed in this policy brief are those of the author(s) and do not necessarily reflect those of the trustees, officers and other staff of the Mohammed Bin Rashid School of Government.

About MBRSG

The Mohammed Bin Rashid School of Government (MBRSG) is a research and teaching institution focusing on public policy in the Arab World. Established in 2005 under the patronage of HH Sheikh Mohammed Bin Rashid Al Maktoum, Vice President and Prime Minister of the United Arab Emirates and Ruler of Dubai, in cooperation with the Harvard Kennedy School, MBRSG aims to promote good governance through enhancing the region's capacity for effective public policy.

Towards this goal, the Mohammed Bin Rashid School of Government also collaborates with regional and global institutions in delivering its research and training programs. In addition, the School organizes policy forums and international conferences to facilitate the exchange of ideas and promote critical debate on public policy in the Arab World.

The School is also committed to the creation of knowledge, the dissemination of best practice and the training of policy makers in the Arab World. To achieve this mission, the School is developing strong capabilities to support research and teaching programs, including:

- Applied research in public policy and management
- Master's degrees in public policy and public administration
- Executive education for senior officials and executives; and,
- Knowledge forums for scholars and policy makers.

Credits and Acknowledgements

Authors: Publications in the PAE series are authored by the respective MBRSG students. The copyright of this publication remain with the author(s).

Acknowledgement:

The following individuals have contributed to this publication

- **Supervisor:** Dr. Saeed Aldhaheri
- **Reviewers:** Lama Zakzak, Fadi Salem and Immanuel Moonesar
- **Production Team:** Engy Shibl | Shuaib Kunnoth

Contact:

For further information about the content of this policy series, please contact the student directly through the identified email address on the cover page.
For general information or comments on the PAE series and publications, please direct emails to:

PAE@mbrsg.ac.ae

كليـــة محمـــد بن راشـــد
للإدارة الحكـــومـــيـــة
MOHAMMED BIN RASHID
SCHOOL OF GOVERNMENT

Mohammed Bin Rashid School of Government

Convention Tower, Level 13, P.O. Box 72229, Dubai, UAE
Tel: +971 4 329 3290 - Fax: +971 4 329 3291
www.mbrsg.ae - info@mbrsg.ae

/mbrsg /mbrsg /company/mbrsg
/+mbrsgae /mbrsgae mbrsgae