

TM



ICDL
Arabia

Cyber Readiness Report 2017/2018

How Ready is the GCC Region with Cybersecurity?



CONTENTS

ABBREVIATIONS	2
ICDL ARABIA, A THOUGHT LEADER ON CYBERSECURITY	3
ACKNOWLEDGEMENTS	4
EXECUTIVE SUMMARY	5
GCC REGION AT A GLANCE	7
METHODOLOGY OF THIS RESEARCH	8
DESIRED IMPACT	9
URGENCY OF CYBERSECURITY IN THE GCC	10
-The Cost of a Cyberattack	11
INTRODUCTION TO CYBERSECURITY READINESS	12
LEGAL MEASURES	14
-Cybercrime Law	14
-Cybercrime Regulation	16
-Cybercrime Training	16
TECHNICAL MEASURES	17
ORGANISATIONAL MEASURES	18
-National Strategy	18
-Governance Model	19
-Responsible Agency/Agencies	20
-Cybersecurity Metrics	21
CAPACITY BUILDING	22
-Public Awareness Campaigns	22
-Cybersecurity Certifications	25
-Web Presence	26
COOPERATION	29
-Multilateral Agreements	29
-Public-Private Partnerships	30
-International NGOs	30
A GLANCE AT ITU'S GLOBAL CYBERSECURITY INDEX	32
-Validation of Cybersecurity Practices	32
-Cyber-Safety of Children	32
CONCLUSION	34
SOURCES	38



ABBREVIATIONS

ADSIC – Abu Dhabi Systems of Information Centre

ADEC – Abu Dhabi Department of Education and Knowledge

CERT – Computer Emergency Response Team

CSIRT – Computer Security Incident Response Team

CPC – Child Protection Centre

GCC – Gulf Cooperation Council

GCI – Global Cybersecurity Index

ICDL – International Computer Driving License

ICT – Information and Communications Technology

ITU – International Telecommunication Union

MoI – Ministry of Interior

NGO – Non-government Organisations

VGT – Virtual Global Taskforce

ICDL Arabia, a Thought Leader on Cybersecurity

ICDL Arabia, formerly known as ICDL GCC Foundation, is the regional arm of ECDL Foundation, a not-for-profit organisation with initial funding obtained from the European Union commission, formed in 1995 by the EU member states national computer societies for the purpose of raising the level of digital skills in the workforce, education and society across Europe.

Building on UNESCO's pioneering role in 2001 with the introduction and operating the ICDL digital literacy certification across the Arab world, ICDL Arabia was then founded in 2004, to become an ICDL operator solely responsible for administering the implementation of ICDL's ICT certification programmes in Bahrain, Kuwait, Oman, Qatar, Saudi, UAE, Iraq and Egypt.

The ICDL ICT certification programmes draw on massive expertise from hundreds of international organisations including, national computer societies, government bodies, as well as educational and training institutions; and local and regional authorities. We collaboratively and regularly work to define the skills and knowledge required to use digital technology effectively, and to empower the masses with the latest trends in ICT skills required in today's workplace, covering topics not just in office productivity applications, but also in Cybersecurity, Social Media, Digital Marketing, Project Planning, Health Information Systems, Computing, and ICT in Education.

For the past five years, ICDL Arabia focused much of its resources on raising the level of Cyber-safety awareness, aimed at teachers, students, and parents. Through its corporate social responsibility, ICDL Arabia invested in various educational development programmes to conquer the online dangers facing our children today. Such dangers include cyber-bullying, Internet addiction, and online exploitation.

Using all its means to draw the attention of policymakers, guardians and other stakeholders on the dire need to take action in support of a safer online world for our children, ICDL Arabia launched a self-funded campaign called OnlineSense. It comprised of several awareness programmes, including advertisements in social magazines, gifts with online safety messages, posters, flyers, and courseware. It also included the development of the first and by far the largest portal, www.onlinesense.org, loaded with free helpful resources in Arabic and English as well as a recently launched YouTube channel loaded with videos in Arabic and English on various important topics pertaining to children's safety online. This is the largest bilingual collection of cyber-safety videos published by any organisation in this region. ICDL Arabia also conducted hundreds of info-sessions at schools, carried out tens of summer camps, and published cooperative research studies annually on the subject of social media and cyber safety – this report being the latest in a series of four 'Cyber Readiness Report 2017/2018'.

The success of ICDL is built on the confidence and trust placed in us by policymakers, governments, and educational institutions from across the world. We closely work with law enforcement agencies and regulators to adopt the best practices in cyber-safety from around the world with local affluence. Today, ICDL Arabia is considered a thought leader and subject matter expert on cyber-safety and is fully committed to contributing to the communities where it operates, providing the latest information and best practices on the subject of cybersecurity, supporting law enforcement, defence, education, government and society as a whole.



ACKNOWLEDGEMENTS

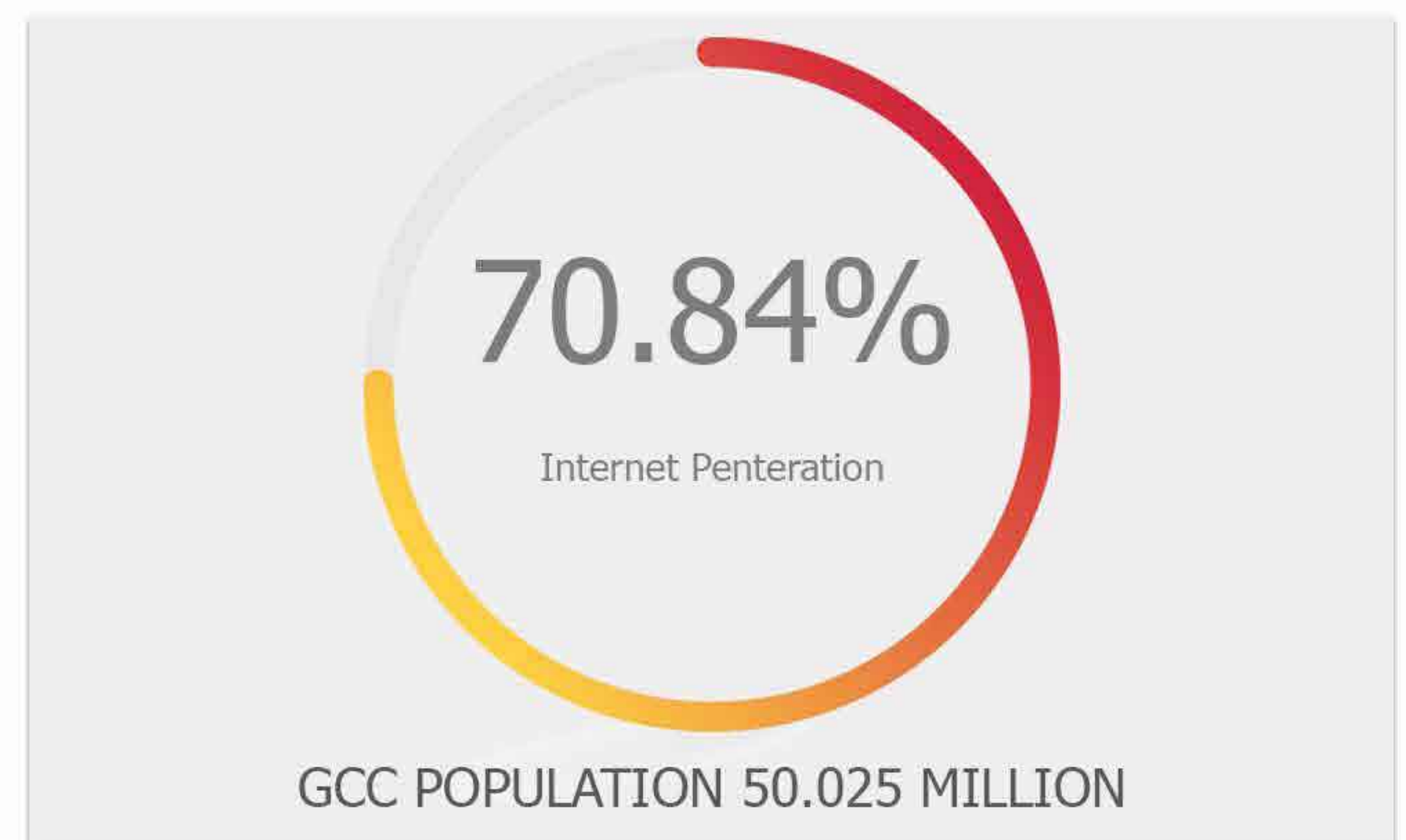
ICDL Arabia would like to acknowledge all of the organisations that participated in providing information and studies cited in this report. These organisations include government entities, organisations in various industries, and other stakeholders.

The following organisations deserve special mention for their contributions:

- The World Bank
- United Nations, the International Telecommunication Union (ITU)
- Potomac Institute for Policy Studies
- Ministry of Information and Communication Technology - ictQatar
- Information Technology Authority - ITA Oman
- HISCOX
- Abu Dhabi Department of Education and Knowledge - ADEC
- Dubai Electronic Security Center - DESC
- UAE Telecommunications Regulatory Authority - TRA
- Oman Police

EXECUTIVE SUMMARY

Internet across the six GCC member states was established between the years 1993 and 1997. Following more than two decades of regulation and investments by the region's governments, corporate citizens, and public-private partnerships, connectivity has expanded exponentially, driving rapid user growth in e-government, e-Learning, e-commerce, e-banking as well as social media.



With more than 35 million internet users in the GCC, most of us today have become dependent on the internet in one way or another. Whether through the use of social media or online apps, people are increasingly relying on technology, creating new business opportunities and stimulating economic growth at unprecedented rates. Consequently, every corner of this region has experienced significant improvements in service delivery, productivity gains, and other forms of innovation.

As in many other countries, the widespread internet usage poses a big challenge to the government as far as cybersecurity is concerned. Policymakers fully realize that increased internet connectivity leads to economic diversification and growth as long as the underlying infrastructure and connected devices remain relatively safe. If governments have economic visions that integrate digital trends with initiatives, it is imperative that preventive measures are considered and aligned with goals to build a robust cybersecurity foundation.

Because technology and the world of digitization evolve so rapidly, policymakers need to regularly gauge their own country's cybersecurity readiness. They need to develop a holistic approach to ensure that their citizens are protected from online financial frauds and other forms of violations. Their cyber readiness strategies need to be translated into stipulated plans of actions.



This year's issue of ICDL Arabia's annual report, 'Cyber Readiness Report 2017/2018', attempts to introduce a fresh perspective on the preparedness of the GCC region in protecting itself from cyber risks. The report further aims to highlight before concerned stakeholders the importance of their participation in the ongoing development of frameworks for the betterment of cybersecurity governance, while working on areas that require investment; not only to possess reliable network infrastructure but also to create a safer and more trusted digital space.



The following stipulations are the main considerations that should be taken into account when developing a national strategy for cybersecurity readiness:

- Expand the national cybersecurity strategy to include the legal, technical, organisational, capacity building [education, training, and awareness], as well as cooperation [public-private partnership, inter-government, foreign-governments collaboration, and general public participation];
- Identify and address current areas of concerns that are potentially slowing down the uptake of internet usage due to mistrust;
- Specify the latest global online trends that could potentially cause harm to the society from misuse, breaches, and hacks.
- Observe, study and compare other governments cybersecurity measures, including the sharing of information relating to new concerns, opinions, and experiences in protecting citizens; and finally
- Adopt proven global standards and best practices to foster a global culture of cybersecurity and ramp up defences against new evolving guises of cyber threats.

GCC REGION AT A GLANCE

Description	 Bahrain	 Kuwait	 Oman	 Qatar	 Saudi	 UAE
Country Population (Million)	1.425	4.053	4.425	2.57	32.28	9.27
Population Growth (Annual)	3.80%	2.90%	5.20%	3.50%	2.20%	1.20%
GDP at market prices (Billion \$)	31.86	114	66.29	152.5	646.4	348.7
GDP Growth (Annual)	2.90%	1.80%	5.70%	2.20%	1.70%	3.00%
Year Internet Introduction	1995	1993	1997	1995	1995	1995
National Cyber Security Strategy	Not Published	Not Published	Not Published	http://bit.ly/2vpnyqv	http://bit.ly/2ij8zbq	Not Published
Internet Domain	.bh	.kw	.om	.qa	.sa	.ae
Internet Users per 100 people	93.5	82.1	74.2	92.9	69.6	91.2
Fixed Broadband & Subscriptions per 100 users	18.61	1.535	5.61	10.116	11.924	12.89
Mobile Cellular subscriptions per 100 users	185.262	231.763	159.861	159.132	179.589	187.348

METHODOLOGY OF THIS RESEARCH

In its research on cybersecurity readiness in the GCC region, ICDL Arabia has considered five main criteria while referencing local and international sources in the process. This report relied on data from the '2017 Global Cybersecurity Index' (GCI) and 'Cyber Wellness Profiles' that were published by the International Telecommunication Union (ITU), a specialised agency of the United Nations responsible for issues pertaining to ICT.

It identifies a number of objectives through measurable criteria and assesses the extent of results achieved. ITU had assessed each country in its report through the following five pillars of cybersecurity readiness.



Legal
Measures



Technical
Measures



Organisational
Measures



Capacity
Building



Cooperation

Relying on its own online research and discoveries from interactions and information provided by the concerned government authorities, ICDL Arabia will present its findings in this report through the above five criteria showing its own assessment of each GCC member state's cybersecurity readiness and the measures taken by each country to promote best practices.

The report will also recommend the scope of improvement in government initiatives to enhance cybersecurity awareness by maximizing on citizens and private sector engagement.

DESIRED IMPACT

Until now, there has been very little GCC-focused research done on cybersecurity readiness. ICDL Arabia aims to draw more attention to this topic and drive early adoption of cybersecurity best practices and innovation in the region.

This report will also attempt to reveal reasons behind countries ranking high and areas where the GCC countries need the most improvement.

We trust that this report will persuade policymakers in the GCC region to re-evaluate their countries' cybersecurity readiness and consider making the necessary budgetary allocations to strengthen cybersecurity.

This also includes bringing in necessary reforms, to enable stakeholders in building better cybersecurity infrastructure to keep citizens safe in the online world.



URGENCY OF CYBERSECURITY IN THE GCC

Over the last 25 years, ICT and the internet have been at the forefront of technological evolution. It has helped transform society into what we now refer to as the Digital Age. Initiatives like e-governance, e-commerce, e-banking, e-health, and e-learning are some among many internet-enabled areas that countries consider crucial to their economic agenda.

Governments continue developing in these areas due to substantial benefits such as efficiency and transparency resulting in faster economic growth and greater public trust. The World Economic Forum cited a 2009 study that estimated a country's GDP would increase by as high as two percent if internet penetration were to rise by 10 percent¹.

Nearly a decade later, the Gulf region has reached a turning point in the Digital Age. The dramatic pace of internet penetration the GCC had witnessed between the years 2000 and 2015 has enabled a majority of people in this region to access the web. Around 226 million people in the Arab region will be logging on to the internet by 2018².

Internet connectivity is becoming less of a problem in this part of the world. What is continuing to increase, however, is the number of cyber threats. **In 2016, 0.7% of all global ransomware detections were in Saudi Arabia, while 0.5% were in the UAE³.**

As the internet grows to contain larger volumes of sensitive information due to higher penetration and online activity, the chances of cybercriminals eyeing this information will get higher. Therefore it is imperative for policymakers to align their economic vision and national security priorities closer to cybersecurity. This will help countries safeguard not only sensitive information, but also prevent online activity that goes against the GCC's cultural values.

The Cost of a Cyberattack:

Cyber threats can come in varied forms such as malware, spyware, ransomware and in current times most of these are associated with data leaks and monetary extortion. This trend is visible from some of the biggest attacks carried out so far this year⁴. Each attack can prove extremely costly for governments, corporations, and individuals.

Types of damage a cyberattack can cause

Revenue loss: According to the 2017 Hiscox Report, cybercrime cost the global economy over \$450 billion in 2016⁵.

Damage to equipment: Damage to electronic equipment connected to the internet through an internal network.

Network outages: Closure/slowdown of local area networks or blockage of access to the internet.



Loss of sensitive data: Over two Billion personal records were stolen in 2016, including millions of medical records⁶.

Blockage in services: Unavailability of websites or other e-services due to malware that block servers.

INTRODUCTION TO CYBERSECURITY READINESS

The fact that no one is cybersecurity ready has been validated by many experts⁷. There are several reasons for this lack of readiness; the primary reason is obvious - rapid technological evolution. As security measures improve; so do cybercriminals' tactics. Ransomware attacks by WannaCry and Petya have proven this.

While we have predominantly referenced the ITU's Cybersecurity Index⁸ in our research, the Cyber Readiness Index (CRI) released by the Potomac Institute for Policy Studies, is also worth a mention here, because the CRI strongly validates the case for cybersecurity readiness built by ITU's research. The CRI also helped spark international discussion and inspired global action against what it calls "cyber insecurity."

The CRI took into account cyber vulnerabilities and possible negative impact of a lack of cybersecurity readiness on economies and objectively evaluated each country's maturity, commitment, and preparedness for cybersecurity and resilience. It recommends measures that countries can take to protect their highly connected economies and safeguard their potential GDP growth by being cybersecurity ready. Mentioned below are the five pillars of cybersecurity readiness that the ITU's research categorically focusses on, and the CRI broadly touches upon⁹.



Legal measures: Has a country demonstrated the commitment for protection against cybercrime?



Technical measures: Does a country have an operational Computer Emergency Response Team (CERT) or Computer Security Incident Response Team (CSIRT)?



Organisational measures: Has a government presented a cybersecurity strategy necessitating a coordinating agency and well-defined indicators for tracking cybercrime?

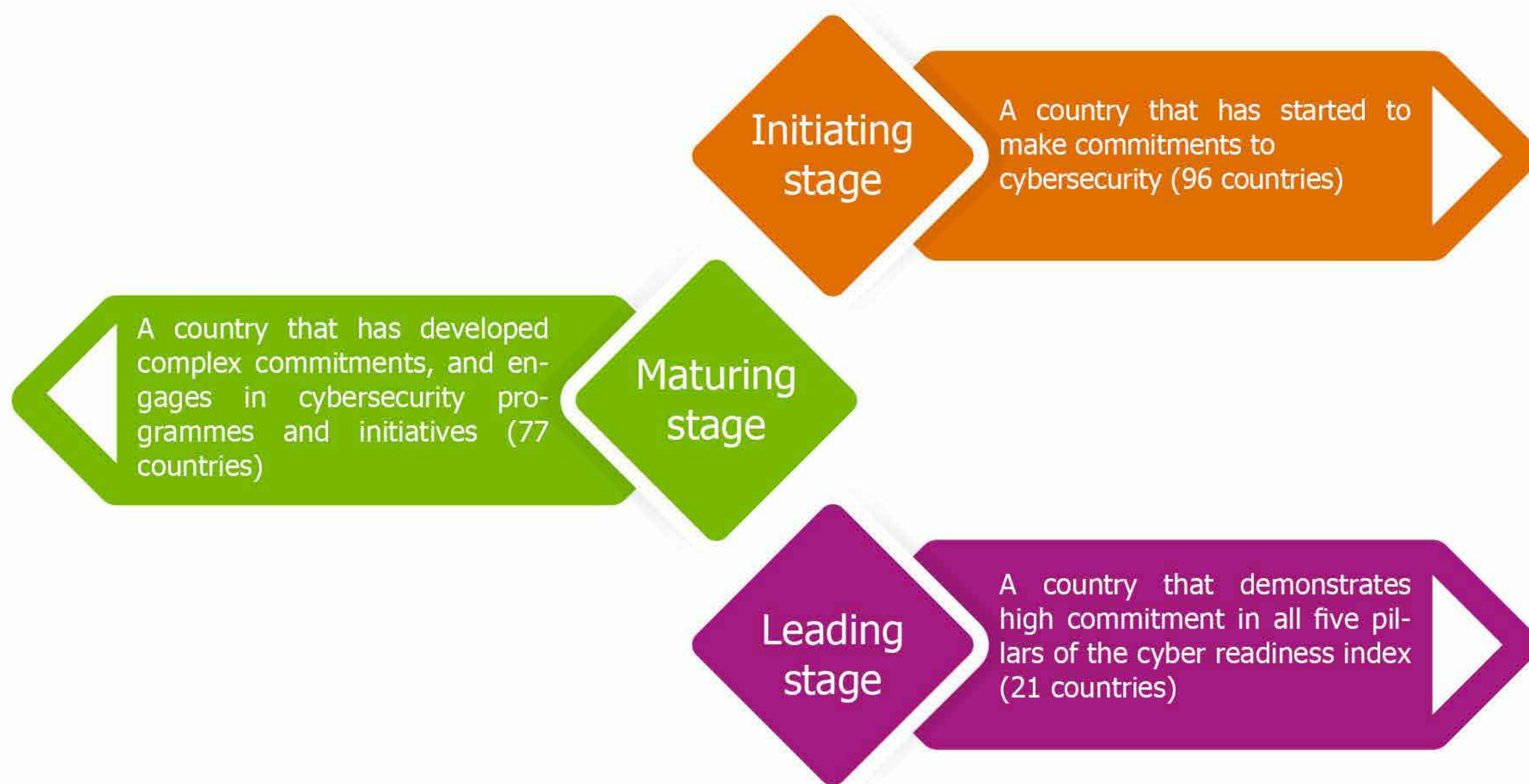


Capacity building: Has a country demonstrated that it is investing in cybersecurity research, providing incentives for the private sector to promote cybersecurity, and/or funding cybersecurity initiatives?



Cooperation: Has a country shown collaborative efforts across national and international domains and between the public and private sectors?

Within these five pillars, there are various indicators through which the ITU has evaluated each country. It asked 'yes' or 'no' questions and categorised countries into the following:



Below is a comparison of GCC countries' overall scores and global ranks:

Country						
	Bahrain	Kuwait	Oman	Qatar	Saudi	UAE
Global Rank	65	139	4	25	46	47
Cybersecurity Maturity	Maturing	Initiating	Leading	Maturing	Maturing	Maturing
Global Cybersecurity Index Score	0.57	0.1	0.87	0.68	0.57	0.57

Oman is the only country in the Leading stage

Qatar, United Arab Emirates, and Bahrain (65th) are in the Maturing stage

Kuwait is the only country in the Initiating stage

Having set a context for the increasing urgency for cybersecurity in the GCC region, here's an analysis of GCC countries' cyber-readiness, based on the five pillars that the ITU uses as key criteria.

LEGAL MEASURES

Legislation is a critical measure to provide a harmonised framework across all sectors of society. To be cyber-ready, providing a legal framework by which the public has to abide is necessary. It also helps set interoperable measures to facilitate international combat against cybercrime and sets the minimum standards of behaviour on how further cybersecurity capabilities should be built. The ITU measures the legal environment based on the existence and number of legal institutions and frameworks dealing with cybersecurity and cybercrime. It includes the following three indicators:

a) Cybercrime Law:







In a highly connected world, cybercrimes can originate from any location and impact multiple countries. Also, unlike conventional crime, cybercrime is not well-defined yet. Therefore, it is of utmost importance for cybercrime laws to be comprehensive. These laws need to list all possible illegal acts, stay up-to-date with new types of crimes, and have an investigative framework capable enough to define, document, and analyse new types of evidence. Laws should be supported by a strong international cooperation framework that can bring perpetrators from any part of the globe to justice. In this section, we have listed existing cybercrime legislations and checked how effective their framework is.

Below are cybercrime laws that are either established or drafted by GCC countries (As compiled by the United Nations Conference on Trade and Development¹⁰):

Country	Title of Legislation / Draft Legislation	Links to Laws
Bahrain	Legislative Decree No. 28 of 2002 with respect to electronic transactions (in Arabic)	http://bit.ly/ICDL2017a
Kuwait	Draft Law on combating Internet Crime	No Link Available
Oman	Royal Decree No. 12/2011 (in English)	http://bit.ly/ICDL2017B
Qatar	Telecommunications Law (No. 34) 2006 (in English and Arabic)	http://bit.ly/ICDL2017C
Saudi Arabia	Law No.79 on Combating Information Technology Crime Law 2007 (in English)	http://bit.ly/ICDL2017D
United Arab Emirates	Federal Law No. 2 on Combating Cyber Crime (in English)	http://bit.ly/ICDL2017E

All GCC countries except Kuwait have cybercrime legislation in place, however, these have to be much more comprehensive, as highlighted in research conducted by Chatham House¹¹.

Below is a comparison of cybercrime

Country						
	Bahrain	Kuwait	Oman	Qatar	Saudi	UAE
Definitions	✓	✓	✓	✓	✓	✓
Criminalisation	✓	✓	✓	✓	✓	✓
Procedural Powers	✓			✓		
Electronic Evidence						
International Cooperation						

General observations based on the Chatham House research.

- **Definitions:** All countries' cybercrime laws clearly define what is considered as cybercrime
- **Criminalization:** All countries' cybercrime laws clearly define acts considered criminal and mention corresponding punishment
- **Procedural powers:** Only Bahrain and Qatar outline a process through which legal powers will be exercised while judging cybercrimes
- **Electronic evidence:** None of the countries comprehensively consider electronic evidence as part of investigation of cybercrimes

b) Cybercrime Regulation:

The GCI points out that Oman is the only country in the GCC, which has well-established cybercrime regulations. While 80% of GCC countries have put in place legislations to curb cybercrime, findings of the GCI clearly indicate that laws alone will not be effective in the region, unless necessary regulations to enforce the laws are put in place.

The GCI cites Oman's cybersecurity regulation as the best example among all countries, globally. **GCC countries can pick best practices from Oman's e-governance framework.** It spells out the rules and procedures, which ensure that government IT projects and systems are sustainable and in compliance with its IT strategies and objectives. This facilitates effective management of IT-related risks.

c) Cybercrime Training:

Law enforcement officials and judicial members need to receive appropriate training on cybersecurity policies as well as the implementation of those laws. Attorneys also need to receive recurring training – preferably with a certification acknowledging when they received the training – since cybercrimes continuously evolve.

ICDL Arabia has not received inputs from government authorities regarding training of lawmakers and lawyers, therefore this aspect has been probed mostly by researching online news and announcements made by government cybersecurity bodies ^(12, 13, 14 and 15).

While government and private entities have announced cyber law workshops, there is no news of training centres dedicated to cyber law. The pace at which cybercrimes are increasing necessitates setting up government-sponsored dedicated cyberlaw training centres that educate not only attorneys but also government officials.

TECHNICAL MEASURES

Without adequate technical measures and the capabilities to detect and respond to cyber-attacks, governments will remain vulnerable to cyber threats. The ITU focuses heavily on technical measures, citing that it is “the first line of defence against cyber threats and malicious online agents¹⁶.” This element is measured based on the existence of technical institutions and frameworks dealing with cybersecurity software endorsed by a country. This includes government and private emergency response teams to identify, defend, and manage cyber threats and enhance security.

Greater budgetary allocations are essential to nurturing cybersecurity response teams and equip them with the wherewithal to counter new attacks. **Experts believe that more investment is needed in infrastructure security across the GCC,** highlighting the cybersecurity threat in the wake of attacks in the past¹⁷.

In addition to response teams, countries need to adhere to internationally recognised cybersecurity standards

for IT practices and software. The GCC will also benefit if it provides cybersecurity certification programmes for government and private sector employees to validate their skills.

ORGANISATIONAL MEASURES

The following are ITU's criteria that measure how effectively a government tackles cyber threats:

a) National Strategy:

A country needs to prioritise cybersecurity and develop a comprehensive set of objectives, policies, and procedural measures to promote security. The policies should be endorsed by all sections of the government and be driven by clear key performance indicators.



The United Kingdom's National Cybersecurity Strategy¹⁸ is a noteworthy example. It provides a context of the trends and opportunities the country acknowledges vis-a-vis technology within a five-year timeframe. It also explains how it will change both public and business behaviours in confidently tackling threats in the digital sphere. The UK has doubled its investment in cybersecurity compared to its previous plan (£1.9 billion).

A similar example of a well-thought-out approach towards cybersecurity is an initiative recently announced by the Dubai government.

The Dubai Cybersecurity Strategy¹⁹ focusses on the following:

- Raise public awareness on the importance of cybersecurity, ensuring building a society that is fully aware of the dangers of cybercrime, as well as developing the skills and capabilities required to manage cybersecurity risks among government and private institutions and individuals.
- Innovate and establish a secure and safe cyberspace characterised by freedom and justice.
- Build a secure cyberspace by establishing controls to protect the confidentiality, integrity, availability, and privacy of data.
- Maintaining the flexibility of the cyberspace (cyber resilience) and ensuring the continuity and availability of IT systems in cyberspace.

Singapore is also a good example. It was ranked #1 in cyber-readiness by the United Nations' International Telecommunications Union²⁰. 60 percent of Singapore's population is confident in its ability to measure the impact of a breach; this is significantly higher than the global average of 47 percent²¹. **GCC countries can also attract much greater participation in building a stronger digital economy by boosting the confidence of the private sector and citizens in protecting themselves online.** Ministries of Interior and Ministries of Education need to work towards making this possible.

b) Governance Model:

A solid national strategy needs to be driven by a roadmap for governance to address challenges and show how policies are put into practice. It also needs to take into account the procedures for sharing confidential information, both within the public sector and between the public and private sectors.

Canada's state government in Ottawa conducted a three-month public consultation²² on updating its cybersecurity strategy. It asked security professionals within the private sector to give their inputs essential to keep country's digital economy strong and secure.

This initiative brought forward new ideas and helped Canada identify gaps and opportunities to shape its approach to cybersecurity. This also strengthened the public's trust in the government while giving them a feeling of involvement.

c) Responsible Agency/Agencies:

The ITU states that cybersecurity governance needs to be carried out by close-knit supervisory bodies such as permanent committees and advisory councils, or cross-disciplinary centres.

Most of these centres should be responsible for surveillance systems, incident responses to cyber-attacks, overseeing the implementation of strategies, and improving organisational structures necessary for coordinating responses to cyber-attacks.

In the GCC region, agencies (Cybersecurity Councils) similar to the ones recommended by ITU can be created and appointed by member countries' respective interior ministries.

A majority of GCC countries are still in the initial stage of forming autonomous bodies dedicated to cybersecurity. While Bahrain, Kuwait and Oman have mandated their Information Technology authority or Telecommunications authority with an additional responsibility of cybersecurity, UAE and Saudi Arabia have established government bodies dedicated to cybersecurity.

In 2012, UAE set up its Intelligence and Signal Authority (NESAs) to work towards "expanding cyber education and creating a collaborative culture rooted in information technology and innovation". In November 2017, Saudi Arabia announced the formation of a National Cybersecurity Authority with the objective of "enhancing the country's cybersecurity to protect its vital interests, national security and sensitive infrastructure".

ICDL Arabia spoke to government representatives from all GCC countries and concluded that attempts to create agencies against cybercrime need much greater impetus. GCC members are either in the process of creating cybercrime centres, or have formed centres that need to put in a greater effort to establish a better equity before the public.

d) Cybersecurity Metrics:

Continuous measurement of cybersecurity initiatives is essential, especially in an atmosphere of rapidly evolving cyber threats. Maintaining cybersecurity metrics will help countries stick to specific standards, both within public and private sectors. These metrics will help determine what IT specialists need to be aware of, how they can improve their technology, and even how they can better stimulate the digital economy as a whole. One country that does this well is the Netherlands. In its National Cybersecurity Centre's annual Cybersecurity Assessment report, it compiles disclosure reports, security advisories and incidents using a registration system²³.

CAPACITY BUILDING

In highly knowledge-reliant economies, cybersecurity can be strengthened by better education in Information Technology. Therefore countries need to develop and strengthen the public's digital skills. The ITU evaluated capacity building through the following: Research and development programmes, public awareness campaigns, educational and professional training courses, certifications (under internationally recognised standards), and incentive mechanisms for companies to train their employees.

ICDL Arabia spoke with GCC government representatives regarding this aspect of capacity building. Below is an overview of programmes and initiatives in GCC countries.

a) Public Awareness Campaigns:

Local governments encourage people to become more cyber aware through campaigns that enhance awareness of certain issues. Almost every GCC country has invested in various projects to engage the public in topics related to cybersecurity and cyber-safety. Some even have government-funded websites dedicated to raising awareness (Refer to the Web Presence section).



AQDAR, a UAE Ministry of Interior (MOI) programme, aims to increase national awareness in preventing crime and educate students about health and safety issues²⁴. Since 2013, it has collaborated with the Ministry of Education (MOE) and ADEC (Abu Dhabi Department of Education and Knowledge) to host cyber-safety awareness sessions addressing all teachers and students. In 2016, Her Highness Sheikha Jawaher Bint Mohammed Al Qasimi, Wife of His Highness the Ruler of Sharjah and Chairperson of the Supreme Council of Family Affairs partnered with ICDL Arabia to conduct awareness sessions for youth and parents.



To contribute to the welfare and safety of the communities where ICDL Arabia operates, it founded OnlineSense to serve as its philanthropic arm with the primary purpose of raising public awareness on cyber-safety. These efforts were carried out through skills programmes and the spreading of awareness messages through digital media.

Since it was founded in 2013, OnlineSense has partnered with a number of government organisations from across the GCC region, launching several wide-scale national projects focusing on digital safety awareness. This included the free distribution of relevant videos and conducting info sessions at more than 2,3000 schools; the publishing of annual studies and analytical reports, such as this, and sharing it with policymakers and stakeholders; carrying out public service awareness campaigns through paid and unpaid ads; and the development of the first bilingual (Arabic and English) website www.onlinesense.org, loaded with the latest resources tools and educational content.



The Sultanate of Oman is very active on cybersecurity and cyber-safety awareness. Oman's National Computer Emergency Readiness Team (OCERT) provides awareness and information security services to the community, government bodies, and private organisations to stay protected from security breaches. OCERT states on its website that it offers Training & Awareness courses, sessions, workshops and conducts events on regular basis to build a stronger culture of cybersecurity²⁵, Early this year, the Ministry of Education had launched an anti-cyberbullying campaign among schools and society; it conducted a roadshow across the country to publicise their campaigns.



The government of Saudi Arabia has formed a non-profit, the Computer Emergency Response Team (CERT), with the aim of increasing and cultivating awareness, knowledge, management, detection, prevention, coordination and response to information security incidence at the national level. CERT states on its website that it promotes awareness on cybersecurity through its portal, and by conducting campaigns and seminars. CERT also publishes latest security alerts, and supports victims of cyber-attacks by analysing incidents and offering recovery strategies.



Q-CERT, Qatar's national information security team is mandated by the Qatar government to safeguard the country's information and communications systems. Q-CERT works with government agencies, businesses, and citizens to address cybersecurity risks, protect sensitive information, and ensure the safety of children on the internet. Qatar's biggest cyber-safety awareness initiative is Keep Them Safe, Keep Them Curious, a campaign highlighting parents' responsibilities to children's online safety.



Bahrain's Central Informatics Organisation (CIO) has set up the Bahraini Computer Emergency Response Team to deal with cybersecurity-related awareness and defence. While the domain name cert.bh has been assigned to Bahrain's CERT, however it is not live. According to Bahrain's Ministry of Information Affairs website, it has conducted awareness sessions for government entities and teachers regarding general internet security rules hosted by eGOV, a programme funded by Bahrain's Ministry of Education. Bahrain's Ministry of Information Affairs also provides web-security courses for its IT employees.



Kuwait's government does not provide any awareness session for its employees. Its Ministry of Education has conducted info sessions for teachers on internet-safety sporadically, but according to government representatives, it has not provided any sessions since 2016.

Need for Improvement in Awareness Initiatives:

While raising cyber awareness is one of the more prominent techniques used within the GCC to engage the public, the countries' investment and effectiveness thereof has been limited. Most campaigns provide generic information and are not consistent in promoting respective initiatives.

Most countries in the GCC do not conduct awareness campaigns on online radicalisation, which is more prevalent in the region compared to other countries.

According to the Centre on Religion & Geopolitics' (CRG) Global Extremism Monitor, around 10,000 people lost their lives due to religious extremist violence (and efforts to counter it) in each quarter of 2016²⁶.

The United Kingdom's government services website provides a counter-extremism strategy that offers in-depth information on countering extremist ideology and building cohesive communities that disrupt and diminish extremist values²⁷.

b) Cybersecurity Certifications:

Within its GCI report, the ITU discusses the significance of certifying public sector professionals and agencies under cybersecurity certification programmes. The certifications should be internationally recognised and have global standards.

The UAE has just begun certifying government professionals in both cybersecurity and cyber-safety related programmes. In 2013, the Dubai Municipality revealed its endorsement of the ICDL Security Certification for its employees. In 2012 Abu Dhabi Systems and Information Centre (ADSIC) and ICDL Arabia collaborated to train and certify thousands of Abu Dhabi government employees including members from Police Force on ICDL's IT Security Certification Programme.²⁸







Need for Improvement in Certification:

Considering that GCC countries are still in the initial stage of building a training framework to equip professionals in cybersecurity, there is a lot to learn from other countries. Germany's Federal Ministry of Education and Research funds the KASTEL competence centre, which offers training²⁹ with a certificate equivalent to a Master's degree in IT security. By comparing professional certification to an academic degree, it ensures governmental sector employees have the skills necessary to thrive anywhere in the IT sector.

In addition to receiving internationally recognised certifications in cybersecurity, governments in the GCC need to provide incentive mechanisms that can establish and expand network foundations in the private sector. This can enhance competitiveness in IT and thereby improve every GCC country's digital economy. Government initiatives can also provide more job opportunities related to ethical hacking and several other domains within a burgeoning cybersecurity market.

c) Web Presence:

Apart from training programmes for professionals, it is critical for governments to have dynamic websites that not only outline the cybersecurity mission, objectives and initiatives but also more critical sections such as cybersecurity alerts, and resources for professionals and the public. Therefore, ICDL Arabia compared GCC countries' cybersecurity websites. Oman, which the ITU has ranked as the world's 4th most cybersecure nation, has a website with various critical sections. ICDL Arabia has therefore used Oman's website as a benchmark to compare with the websites (or web documents in the absence of a website) of other GCC countries.

Country (Website Linked)						
	Bahrain	Kuwait	Oman	Qatar	Saudi	UAE
Mission, Vision, & Objectives	✓		✓	✓	✓	✓
Training Initiatives	✓		✓	✓	✓	
Awareness Initiatives			✓	✓	✓	✓
Report Incident			✓	✓	✓	✓
Proactive & Reactive Services			✓	✓	✓	✓
Free Vulnerability			✓	✓	✓	
List of Latest Alerts			✓	✓	✓	✓
News and Events	✓		✓	✓	✓	✓
Technical Literature on Cyber-Security			✓	✓	✓	✓
Mention of International Collaboration & Public Private Partnerships	✓		✓	✓	✓	

Note: While some countries have a few of these sections sporadically available through various government websites, we have picked up one website most closely associated with the cybersecurity of a country to check if that website has the sections. The idea is to highlight the importance of countries to have a one-stop repository of all aspects of cybersecurity.



Oman, Saudi Arabia, and Qatar have the most comprehensive websites covering all vital aspects of cybersecurity



UAE's website has a moderate scope to become more comprehensive, while Bahrain's website has a wide scope to become more comprehensive



Kuwait does not have a website dedicated to cybersecurity



Bahrain's website has the most engaging awareness content comprised of videos, illustrations, and articles



COOPERATION

The final component mentioned in the GCI relates to partnerships between the public and private sectors. Cybersecurity requires input from all sectors and disciplines and for this reason needs to be tackled from a multi-stakeholder approach. Cooperation does not just require dialogue, but it improves coordination between sectors and enables the creation of a more comprehensive and effective strategy within a nation state. It can also help enable better development of cyber-related capabilities and allow for better investigation of cybercrimes.

GCC countries have a long way to go in collaborating better for cybersecurity³⁰. Here are a few collaborative efforts GCC governments can emulate, across national and international domains and between public and private sectors.

a) Multilateral agreements:

Having official partnerships with fellow GCC countries can facilitate collaboration between countries and help uphold internationally recognised standards for the entire region. For example, the Nordic region (Denmark, Finland, Iceland, Norway, and Sweden) collaborate through the Nordic National CERT Collaboration. This includes technical cooperation³¹ and cybersecurity exercises to assess and strengthen cyber readiness, examine incident response processes and enhance secure information sharing in the region. The GCC would benefit greatly by collaborating with one another. Not only would it reinforce existing relationships within the community, but it would strengthen communication efforts about cyber threats. With the proper infrastructure of a regional CERT, countries within the alliance would be able to respond to cyber-attacks quicker while minimizing damage. In fact, the Swedish Civil Contingencies Agency confirmed that there is a “need for information sharing, collaborating, and shared situational awareness during a critical cyber incident impacting Nordic nations.³²” If a GCC country were impacted by a ransomware attack such as WannaCry or NotPetya, it would certainly be easier to warn others in the region and be more effectively transparent with the public.



b) Public-Private Partnerships:

Public-Private Partnerships (PPP) refer to exchange of information between the public and private sectors. These efforts help foster anti-fraud, anti-phishing, and external vulnerability testing.

It is essential for big data handlers like Facebook and Google to work with government entities, particularly for Ministries of Interior. As part of investigations, government officials request data about people who use their services. The vast majority of these requests relate to criminal cases, but authorities can also request private companies to restrict access to content in an effort to eliminate anything that violates local laws³³.

Companies like Facebook have made information about the number of government requests for user-related data public. Government requests for Facebook account data increased by 9% globally³⁴ compared to the first half of 2016, from 59,229 to 64,279 requests. UAE has made the most number of requests for Facebook user data since 2013, followed by Kuwait. Other GCC countries have comparatively much lesser number of requests. All these requests were made for government investigation of crimes (cybercrimes and other crimes).

c) International NGOs:

Non-government Organisations (NGO) are emerging as governments' important cybersecurity allies. These bodies encourage countries to participate in international projects, cyber-related events, and gather expert from all over the world to help train government officials in sharing vital information. A few countries in the region have sought to form global partnerships with organisation that specialise in the subject of cyber-safety.



UAE's Child Protection Centre (CPC), an authority working within the interior ministry, joined Virtual Global Taskforce (VGT) to leverage international experience and practices in combating child online sexual abuse. Early 2014, CPC and ICDL Arabia have joined forces to build a safer environment for children and protect them from becoming victims of online abuse. CPC aims at achieving its goal by seeking compliance to Internationally-accepted child protection standards, enhancing awareness through community outreach programmes, and offering legal services. CPC has introduced a hotline (116 111) that can be contacted to report online and offline abuse³⁵ of children residing in the UAE.



The VGT is an international NGO that seeks to build an effective, international partnership of law enforcement agencies, non-government organisations and the private sector to help protect children from online child abuse and other forms of transnational child sexual exploitation. The UAE joined the VGT in 2010 and has been its chair since 2015³⁶.



A GLANCE AT ITU'S GLOBAL CYBERSECURITY INDEX

While the ITU's GCI touches upon many important aspects of cybersecurity readiness, there are a few areas of improvement, which might have had an impact on the accuracy of its findings on the GCC region.

a) Validation of Cybersecurity Practices:

GCI has noted that Qatar has a Cybercrime Investigation Centre to "safeguard the public and crack down on those who use technology to carry out criminal activities." Aside from a press release in early 2016 discussing a new location³⁷, very little information has been written about what the centre does to prevent cybercrimes. In fact, there is very little proof that the centre is active. After speaking with government representatives of Qatar, ICDL Arabia has found that the cybercrime law that was adopted has not been enforced yet. The ITU report still highlighted this as one of the reasons why Qatar is one of the top three cyber-ready countries in the region.

b) Cyber-Safety of Children:

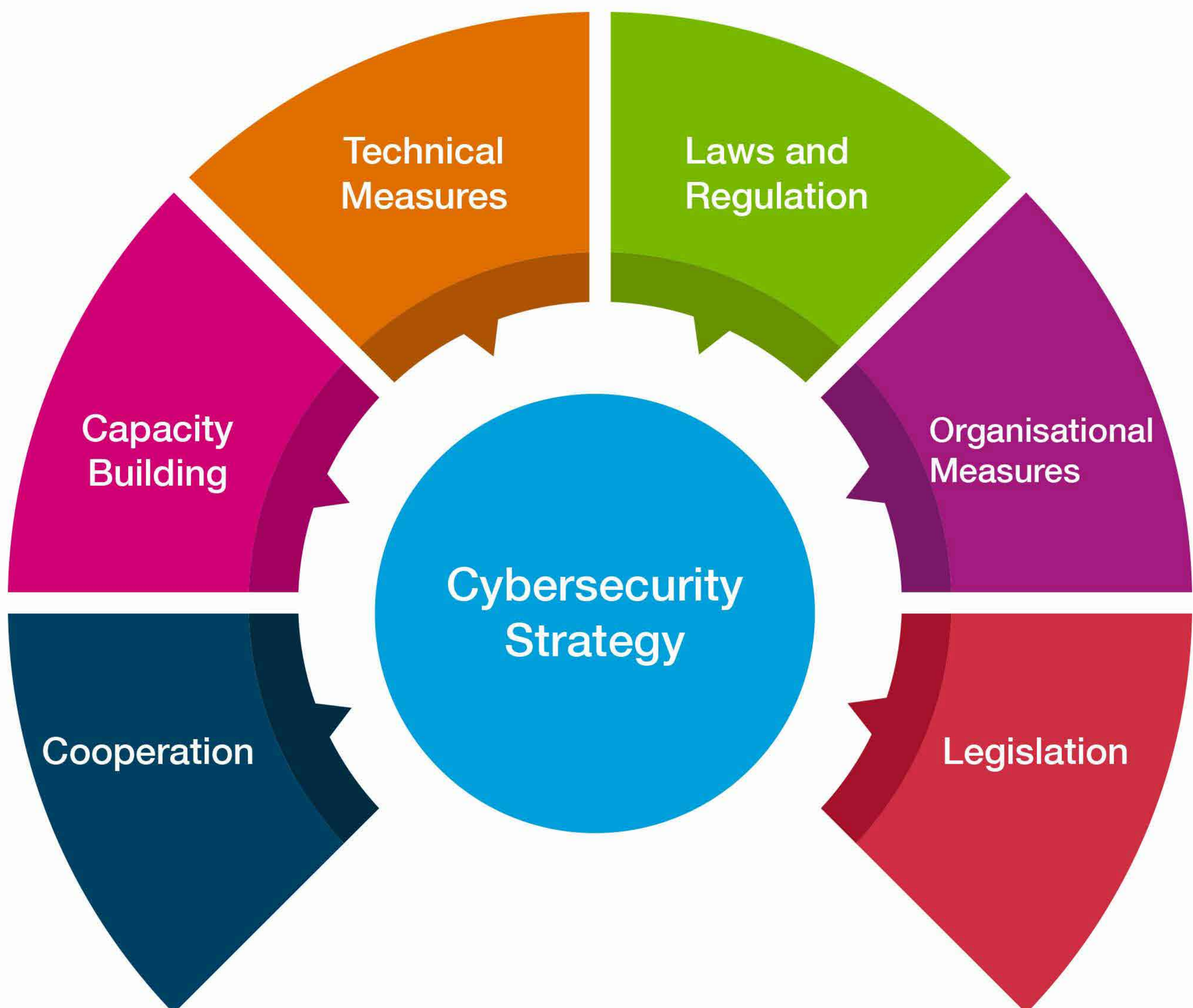
In addition to the lack of qualitative measurement, very little discussion about cyber-safety is incorporated in the ITU's analysis. Although the questionnaire talks about child online protection in its Legal pillar, it does not provide disclosure of their definition of child online protection nor does it provide any discussion for how ITU measures child online protection. It is not mentioned anywhere in the ITU report what steps government entities have taken to increase awareness in schools or within the household. Most cyber readiness research can go deeper into the differences between cybersecurity and cyber-safety. Institutionally, both are extremely important to maintain a safe and prosperous economy. While cybersecurity primarily refers to the state of being protected against criminal or unauthorised use of online data, cyber-safety refers more to how to use information technology safely and responsibly.

In other words, cybersecurity includes more technical aspects and cyber-safety contains more educational and social aspects such as cyberbullying, cyber exploitation, and the online radicalisation of children. These topics were ignored in the ITU's report, and thereby affected the countries' overall rankings and their rankings within the region. There are several ways in which governments should incorporate cyber-safety into a cybersecurity readiness report.

For instance, in the Capacity Building section of future ITU reports, education ministries could be asked whether they offer public awareness campaigns on cyber-safety. ITU could have also investigated whether countries do provide mandatory training, workshops, info sessions, courses, and/or certifications for teachers about cyber-safety. One might be able to rank countries based on how secure the systems are, but one cannot truly determine how cyber-ready a government or society is without the inclusion of cyber-safety education. ITU has been contacted by ICDL Arabia several times to respond to questions triggered by their Global Cybersecurity Index for 2014 and 2017, and to learn more about their findings outlined in the report and the criteria used to rank the readiness of the Arab states, but unfortunately no one had reverted back to ICDL Arabia at the time of publishing this report.

CONCLUSION

This report acknowledges that countries in the GCC region have started to consider cybersecurity as an important part of national security and digital economy. However, **there is still a big disparity between GCC nations as far as cybersecurity readiness is concerned. While Oman ranks among the world’s top four countries in cybersecurity, Kuwait is almost at the bottom of the list, at 139.** This disparity reveals the urgent need for GCC countries to adopt a collaborative approach to develop a solid foundation for cybersecurity, with a thorough strategy at the core.



Here is a summary of immediate measures this report recommends for countries to start with:

- Prioritise GCC-level collaboration and knowledge sharing to develop detailed cybersecurity strategies. Emulate evolved models such as the UK's cybersecurity strategy³⁸ and learn from the approach adopted by regional examples such as the Dubai cybersecurity strategy³⁹.
- Set up a cybersecurity lab to keep track of the latest threats and devise ways of tackling those.
- Educate attorneys about the latest cyber threats, and build a comprehensive law against online fraud and violations. Follow a benchmark such as the US Cybersecurity law⁴⁰ necessary to tackle latest cybercrimes.
- Establish government centres for cybersecurity training of employees in the public and private sectors working on critical infrastructure that need protection. Training initiatives carried out in Wales⁴¹ are a good example.
- Forge agreements with countries from which the majority of cyber-crimes are originating to effectively prosecute criminals from those locations. Start by collaborating with international cybersecurity organisations⁴².
- Make government cybersecurity websites more comprehensive, with updates, alerts, resources, security services, and training programmes.

As we conclude this report, it is important to consider the following:

Cyber Readiness Encompasses More than Cybersecurity:

The term cyber-readiness has almost become synonymous with cybersecurity readiness, but it is important to distinguish between the two. Cyber-readiness has a much wider scope than just cybersecurity; it refers to everything essential for a country to be ready for the cyber world. It has in its ambit the entire sphere of digital infrastructure, information technology skills, internet penetration, awareness, and security essentials for countries to leverage the cyberspace for development.

Transparency is the Hidden Sixth Element of Cybersecurity Readiness:

In the cyberspace a security breach can take place anywhere, people's involvement is critical to identify cyber-attacks and contain those in the initial stage. The public will be involved only if the government fosters confidence through transparency and dialogue. Here are a few examples of what governments should share with people to build a transparent environment:

- Measures taken by the government to protect people's privacy and civil liberties in cyberspace.
- Announcement of cyber-attacks on government/private networks and sensitive information might impact the public's interests.
- The government's approach, capabilities, and initiatives to identify and counter cyber attacks.

Further (Local) Cyber Readiness Research Needs to Be Conducted and Collected

ICDL Arabia's interaction with GCC government representatives for the purpose of this report revealed that countries in the region do not have adequate data to determine cybersecurity readiness. Studies conducted by -Kaspersky Lab⁴³ and the ITU⁴⁴ have highlighted a lack of cybersecurity readiness and awareness in the GCC.

However, **ICDL Arabia did not come across any report on cybersecurity readiness published by any government in the region. This indicates a possible lack of government-led research on this urgent topic.** Taking stock of cybersecurity preparedness is the first step towards initiating measures to become more secure. Therefore, countries in the GCC region should conduct state-supported research to know more about the latest threats, and capabilities to tackle those threats. Undoubtedly, cybersecurity is essential to a nation's digital future and its national security.

The success or failure of a country's cybersecurity readiness critically depends on the ongoing direct engagement of a government supported by proper funding, policies and awareness programmes. As governments of the GCC pursue to diversify their economies, they will need to nurture ICT uptake by citizens. It equally has to commit to increasing the safety and resilience of its internet infrastructure from all kinds of risks, including data breaches, criminal activities, service disruptions, and property destruction. It is simply this - the more trust that is placed by citizens when transacting online, the higher the returns are for a nation.

SOURCES

1. http://www3.weforum.org/docs/WEF_IT_DynamicEcosystem_Report_2009.pdf
2. <http://www.arabianbusiness.com/arab-internet-users-forecast-rise-226m-by-2018--626635.html>
3. <http://www.itp.net/mobile/612536-in-the-uae,-one-in-136-emails-is-malicious-research>
4. <https://www.wired.com/story/2017-biggest-hacks-so-far/>
5. <https://www.hiscox.co.uk/cyber-readiness-report/docs/cyber-readiness-report-2017.pdf>
6. <https://www.hiscox.co.uk/cyber-readiness-report/docs/cyber-readiness-report-2017.pdf>
7. https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CyberReadiness_EN.pdf
8. https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CyberReadiness_EN.pdf
9. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01--2017-PDF-E.pdf
10. http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx
11. <https://www.chathamhouse.org/sites/files/chathamhouse/publications/research/2017-06-30-cybercrime-digital-economy-gcc-hakmeh.pdf>
12. <http://www.bna.bh/portal/en/news/762914>
13. <https://www.tra.gov.ae/en/media-hub/press-releases/2017.1.15/tra-hosts-the-first-introductory-workshop-of-the-uae-information-security-awareness-committee-isa.aspx>
14. http://marinafox.com/news/training_for_lawyers_on_cyber_law
15. <https://www.theknowledgeacademy.com/sa/courses/cyber-security-training/cyber-security-awareness/riyadh/>
16. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf
17. <http://saudigazette.com.sa/article/152682/?page=1>
18. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf
19. <http://www.dubai.ae/en/Pages/DCSS.aspx>
20. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017PDF-E.pdf
21. https://www.accenture.com/t20170406T010037__w_/sg-en/_acnmedia/PDF-38/Accenture-Facing-Cybersecurity-Conundrum-Singapore.pdf
22. <http://www.itworldcanada.com/article/breaking-news-ottawa-announces-public-consultation-on-cyber-security-strategy/385740#ixzz4dm1Qjsu>
23. <https://www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands/cyber-security-assessment-netherlands-2016.html>
24. <http://www.aqdar-uae.com/en/about/>
25. <http://www.cert.gov.om/services.aspx>
26. <http://www.religionandgeopolitics.org/global-security/extremism-and-conflict-what-watch-2017>
27. <http://www.gov.uk/government/publications/counter-extremism-strategy>
28. https://icdlarabia.org/uploads/news/english/2012/Sep/ADSIC_Security_Eng.pdf
29. <http://www.kastel.kit.edu/>
30. <https://www.thenational.ae/business/technology/gcc-urged-to-coordinate-cyber-security-following-wannacry-attack-1.90087>
31. <http://www.msb.se/en/Tools/News/Nordic-cyber-security-exercise-was-conducted-in-Linkoping/>
32. <http://www.msb.se/en/Tools/News/Nordic-cyber-security-exercise-was-conducted-in-Linkoping/>
33. <https://govtrequests.facebook.com/about/>
34. <https://newsroom.fb.com/news/201704//global-government-requests-report-7/>
35. https://icdlarabia.org/uploads/news/english/2015/UAE_Welcomes_ICDL_Arabic_to_Virtual_Global_Taskforce.df
36. <https://www.moi.gov.ae/en/media.center/News/News4k20151111.aspx>
37. <https://www.moi.gov.qa/site/english/news/2016/01/-24/-35540.html>
38. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf
39. <http://www.dubai.ae/en/Pages/DCSS.aspx>
40. <https://fas.org/sgp/crs/natsec/R42114.pdf>
41. <http://www.computerweekly.com/feature/How-Wales-has-evolved-into-a-hotspot-for-cyber-security>
42. <https://www.thebalance.com/leading-information-security-organizations-2071545>
43. https://me-en.kaspersky.com/about/press-releases/2017_kaspersky-labs-latest-parental-control-report-shows-uae-kids-online-behavior
44. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf