Measuring Cloud Readiness

Maurice Danaher, Saif Al Rumaithy

***Abstract*—**Over the past few years there has been a huge movement to cloud services by businesses, consumers and governments. Cloud technology is significantly changing the IT landscape with users assessing a wide range of IT services provided by cloud service providers via the Internet. There is much evidence that points to the importance of cloud computing for global growth. The move to cloud computing is accelerating, but some observers and researchers have produced evidence that shows that the policy environment in some countries is not improving sufficiently to support this rapid expansion. Further, countries that lag behind in their policy environment hamper not only their own users but global expansion as a whole. Researchers have developed a scorecard system which can be used to measure "cloud readiness" for a country. It examines seven policy categories and also considers ICT infrastructure. It was used by the developers to investigate the cloud readiness in studies that covered 24 countries. In the project described here the method is presented in detail and it has been used to examine the UAE and show how it compares with the other 24 countries. The scorecard consists of 66 questions, each of which was researched.

***Keywords*—**cloud computing, cloud services, cybercrime, privacy, security

I. Introduction

Computing on the cloud means storing and accessing data and programs over the Internet rather than on one's own system. The cloud is a virtualization of resources such as servers and other computers, networks, applications, data storage and services to which the end user has on-demand access [1]. The systems are configured in such a way that they can be shared by many organizations or individuals. Cloud services are provided to the user without the need for the user to have any knowledge of the underlying systems. Such "on-demand" technology saves funds on hardware, system management, server maintenance, and fees paid to purchase licenses [2]. Cloud technologies have made it possible to optimize various aspects of organizational, computational, governmental, educational, and business processes by providing access to significant and yet comparatively low cost data-processing capabilities. Additionally the technology typically allows access using any device from any location facilitating an increasingly mobile workforce.

An important impact of cloud computing globally is its potential to offer millions of jobs through small and medium-sized companies and generate billions of dollars in revenues [3]. A study in 2012 by IDC [4] predicted that around 14 million jobs would be created worldwide and $1.1 trillion in revenue would be generated by 2015. This global growth though is dependent upon an increasingly supportive environment being provided by governments and industry.

According to a 2013 research study by BSA-The Software Alliance [5] reflecting wide research on international cloud computing implementation, "cloud readiness" is improving. Cloud readiness refers to the policy environment in the country to support growth in cloud computing. BSA-The Software Alliance is a leading advocate for the global software industry before governments and in the international marketplace. In a major study to analyze the level of preparedness of a country to support and promote the growth of cloud computing they developed a methodology based on a scorecard approach. The scorecard measures "cloud readiness" by examining seven policy categories and by considering information and communication technologies (ICT) infrastructure.

BSA [5] conducted a study of 24 countries that together account for 80% of the world's market for ICT. The study showed quite clearly, as would be expected, that the advanced economies were quite well prepared in comparison to the developing countries. In the developing countries the study showed that although there are some areas where the policies are supportive, there's still a lot to be done and issues to be resolved in order to establish stable, highly-convenient, internationally accepted, well-coordinated services which would be able to improve government, educational, and business processes. Some developing countries, for example, have restrictive policies such as trade limitations, or complex bureaucratic processes, which hinder cloud computing.

The United Arab Emirates is one of the world's most rapidly developing countries. It is quick to embrace technology and an ever increasing number of users are adopting cloud computing [6]. According to Chen [7] the unique social, political, and cultural environment of UAE significantly shapes the local ICT practice and business directions. In the research reported here the BSA methodology was used to study cloud readiness in the UAE. The results of study show the current situation in the UAE and how the country compares with 24 other nations.

II. BSA Scorecard

The BSA Scorecard [5] considers regulations and laws in relation to cloud computing in seven policy categories and it also considers each country's ICT infrastructure. The seven policy categories are the areas which the BSA researchers maintain are of primary importance in order to support the growth of cloud computing. They are: (1) data privacy, (2) security, (3) cybercrime, (4) intellectual property, (5) support

for industry-led standards and international harmonization of rules, (6) promoting free trade, and (7) ICT readiness and broadband deployment. Each of these areas is briefly described below and its relevance and importance to the UAE is discussed.

A. Data Privacy

Being one of the core expectations of cloud users, information privacy is of the utmost importance for cloud computing to gain nation-wide and world-wide support. Individual and enterprise users need to be assured that their private data is safely stored and protected. An investigation carried out in 2011 showed that not more than 2% of European companies had taken the risk to implement "Infrastructure as a Service" cloud computing because of potential privacy threats [8]. A major concern about data privacy is based on the fact that with cloud computing sensitive data is stored outside of an organization and maybe country as well and therefore the data faces risks beyond the owner's control.

According to Weber [2] "family and individual privacy are important cultural values in the Arabian Gulf." In the UAE individual, family, and national dignity are treated as factors of significant importance. Therefore data privacy issues, if not resolved properly, will remain a major obstacle to cloud computing implementation for organizations and individual users in the Arabian Gulf.

B. Security

There are numerous security concerns that must be considered in cloud computing. [9],[10],[11]. These include: data owners not having control of the computer systems on which their data resides; users are totally dependent on the service provider for security; service problems could affect the user's business; the service provider may not use cutting edge cyber security. Basically it can be said that data residing on computer systems owned and managed by another entity may not be as safe as if the data is maintained on a user's own systems.

A recent study in the UAE [12] showed that users have a strong belief that cloud computing is intrinsically insecure. The vast majority of users believed that they could not trust cloud providers to keep their data secure. Clearly if cloud computing is to have more acceptance in the UAE then work needs be done to build trust in the security of the services.

C. Cybercrime

Cloud computing service providers store huge amounts of client data in their data centers and thus present a tempting lucrative target for criminals. Cloud providers, industry and governments around the world agree that cybercrime is a huge threat. Individuals and organizations fear that their sensitive information may be accessed and used by competitors or criminals. To fight cybercrime comprehensive laws must be in place which provide a meaningful deterrent and clear causes of action. The legal system should facilitate effective enforcement of the laws.

In the UAE laws to address cybercrime were introduced in 2006 and later extended in 2012. In 2014 the UAE's newly established National Electronic Security Authority (NESA) announced new strategies and policies to safeguard the country's digital space [13].

D.Intellectual Property Rights

Appropriate laws have to safeguard authorship, support and protect research and development, and enforce violation penalties. Developers and providers of cloud technology must have strong protection for their investment. Cloud providers must operate under clear laws that guide them on how to act when users breach copyright. Additionally there should be a serious effort to enforce IP laws. Many developing countries introduce copyright laws yet make little effort to enforce the laws.

UAE signed the World Intellectual Property Organization (WIPO) Copyright Treaty in 2004 concerning the matters of copyright, and enforcement of intellectual property rights. The WIPO's goal is the development and implementation of a balanced intellectual property system to stimulate international economic growth and safeguard copyright.

A. Support for Industry-led Standards & International Harmonization of Rules

In order to have smooth flow of data between cloud providers and around the world significant efforts are required to promote interoperability and openness. Users need to have interoperability and thus industry are engaged with standards development organizations to create appropriate standards. Governments should support this work by collaboration with industry in standards development and by minimizing conflicting legal obligations on cloud service providers.

The UAE government supports industry-led standards in many technology areas and engages with other countries in discussions on regulations.

B. Promoting Free Trade

Free trade implies the absence of borders in relation to business processes and communication. Free trade makes it possible for example for a company to have foreign ownership, repatriate its profits, support international partnerships, and provide services worldwide. Berry & Reisman [14] explain positive potential of free trade agreements. For example, the U.S. – Korea Agreement states that "Parties shall endeavor to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders." Free trade agreements and partnerships provide an opportunity to develop cloud computing services by establishing cross-border information flows. Restrictive trade policies create barriers that hamper the growth of cloud computing.

In the UAE the government sponsored UAE Free Zones organization promotes the development of ICT in the country.

C. ICT Readiness, Broadband Deployment

In order to stimulate cloud computing use by individuals and business there must be a good ICT infrastructure. Access costs should be attractively priced, and speeds and reliability should be high so that the service is appealing to subscribers and potential subscribers.

The UAE has already invested significantly in high-speed broadband internet access, and according to a 2014 report was ranked 2nd among Arab states for ICT implementation [15].

H Methodology of the Scorecard

The scorecard is designed such that the policy environment of a country is examined in the seven categories described above by researching and analyzing a total of 66 questions. The categories are weighted as shown in Table 1 and within every category each question is weighted. The total for all questions sums to a maximum value of 100.

Table I. Scorecard weight distribution

CATEGORY	WEIGHT
Data Privacy	10%
Security	10%
Cybercrime	10%
Intellectual Property Rights	20%
Support for Industry-Led Standards & International Harmonization of Rules	10%
Promoting Free Trade	10%
ICT Readiness, Broadband Deployment	30%

The questions are generally framed so as to be answerable by "Yes", "No" and "Partial". BSA explain the meaning of the answers as [5, p.13] "Yes indicates a positive assessment, which is generally considered to be an encouraging step towards the establishment of a favorable legal and regulatory environment for cloud computing. No indicates a negative assessment and the presence of a potential barrier to the establishment of a favorable legal and regulatory. Partial indicates that the assessment is positive in part, although some gaps or inconsistencies may exist which require further remedial work." Some questions require explanatory answers.

III. UAE Data

Data was collected in all categories in order to address all questions on the scorecard. This involved researching an extensive range of resources. To acquire information about data privacy, security and cybercrime, related national legislation and regulations and associated publications were carefully reviewed and studied. Additionally various bodies were approached to elicit information including the UAE's National Electronic Security Authority and the UAE's Computer Emergency Response Team. The categories of intellectual property, industry standards and free trade were researched by studying legislation, rules and regulations and related publications. Additionally a number of industry bodies were interviewed. Information on ICT was gathered from various published reports, from interviews with the local ICT providers and from the Telecommunications Regulatory Authority. There were a few questions to which answers were not determined. As this work is ongoing answers may be obtained in the near future, however their impact is minimal on the overall result as the score for each of those particular questions would be close to zero. The results of the research for each of the 66 questions are shown in Table 2.

Table II. Research Questions

DATA PRIVACY	
1. Are there laws or regulations governing the collection, use, or other processing of personal information?	Yes
2. What is the scope and coverage of privacy law?	By sector
3. Is the privacy law compatible with the Privacy Principles in the EU Data Protection Directive?	Partial
4. Is the privacy law compatible with the Privacy Principles in the APEC Privacy Framework?	Partial
5. Is an independent private right of action available for breaches of data privacy?	Available
6. Is there an effective agency (or regulator) tasked with the enforcement of privacy laws?	None
7. What is the nature of the privacy regulator?	Not applicable
8. Are data controllers free from registration requirements?	Yes
9. Are cross-border transfers free from registration requirements?	No
10. Is there a breach notification law?	No
SECURITY	
1. Is there a law or regulation that gives electronic signatures clear legal weight?	Yes
2. Are ISPs and content service providers free from mandatory filtering or censoring?	No

3. Are there laws or enforceable codes containing general security requirements for digital data hosting and cloud service providers?	Limited coverage in legislation
4. Are there laws or enforceable codes containing specific security audit requirements for digital data hosting and cloud service providers?	No data
5. Are there security laws and regulations requiring specific certifications for technology products?	No data
CYBERCRIME	
1. Are cybercrime laws in place?	Yes
2. Are cybercrime laws consistent with the Budapest Convention on Cybercrime?	Partial
3. What access do law enforcement authorities have to encrypted data held or transmitted by data hosting providers, carriers, or other service providers?	Access with a warrant
4. How does the law deal with extraterritorial offenses?	Comprehensive coverage
INTELLECTUAL PROPERTY RIGHTS	
1. Is the country a member of the TRIPS Agreement?	Yes
2. Have IP laws been enacted to implement TRIPS?	Yes
3. Is the country party to the WIPO Copyright Treaty?	Yes
4. Have laws implementing the WIPO Copyright Treaty been enacted?	Yes
5. Are civil sanctions available for unauthorized making available (posting) of copyright holders' works on the Internet?	Yes
6. Are criminal sanctions available for unauthorized making available (posting) of copyright holders' works on the Internet?	Yes
7. Are there laws governing ISP liability for content that infringes copyright?	No
8. Is there a basis for ISPs to be held liable for content that infringes copyright found on their sites or systems?	Yes
9. What sanctions are available for ISP liability for copyright infringing content found on their site or system?	Not applicable
10. Must ISPs take down content that infringes copyright, upon notification by the right holder?	No
11. Are ISPs required to inform subscribers upon receiving a notification that the subscriber is using the ISP's service to distribute content that infringes copyright?	No
12. Is there clear legal protection against misappropriation of cloud computing services, including effective enforcement?	Limited protection
SUPPORT FOR INDUSTRY-LED STANDARDS & INTERNATIONAL HARMONIZATION OF RULES	
1. Are there laws, regulations or policies that establish a standards-setting framework for interoperability and portability of data?	No data
2. Is there a regulatory body responsible for standards development for the country?	Yes
3. Are e-commerce laws in place?	Yes
4. What international instruments are the e-commerce laws based on?	UNCITRAL Model Law on ecommerce
5. Is the downloading of applications or digital data from foreign cloud service providers free from tariff or other trade barriers?	Yes
6. Are international standards favored over domestic standards?	No data
7. Does the government participate in international standards-setting process?	Yes
PROMOTING FREE TRADE	
1. Are there any laws or policies in place that implement technology neutrality in government?	No data
2. Are cloud computing services able to operate free from laws or policies that mandate the use of certain products (including, but not limited to, types of software), services, standards, or technologies?	Yes
3. Are cloud computing services able to operate free from laws or policies that establish preferences for certain products (including, but not limited to, types of software), services, standards, or technologies?	Yes

4. Are cloud computing services able to operate free from laws that discriminate based on the nationality of the vendor, developer, or service provider?	Yes
ICT READINESS, BROADBAND DEPLOYMENT	
1. Is there a national broadband plan?	Yes
2. Are there laws or policies that regulate the establishment of different service levels for data transmission based on the nature of data transmitted?	No data
3. Base Indicators	
3.1. Population (2011)	8,442,000
3.2. Urban Population (%) (2011)	84.4%
3.3. Number of Households (2011)	No data
3.4. Population Density (people per square km) (2010)	94.4
3.5. Per Capita GDP (US$ 2011)	$37,797
3.6. Public Cloud Services Market Value (2011) (Billions of US$)	No data
3.7. Personal Computers (% of households) (2011)	76%
4. ICT and Network Readiness Indicators	
4.1. ITU ICT Development Index (IDI) (2011) (Score is out of 10 and includes 161 countries)	5.64
4.2. World Economic Forum Networked Readiness Index (NRI) (2012) (Score is out of 7 and includes 142 countries)	4.77
4.3. International Connectivity Score (2011) (Score is out of 10 and includes 50 countries)	No data
4.4. IT Industry Competitiveness Index (2011) (Score is out of 100 and includes 66 countries)	No data
5. Internet Users and International Bandwidth	
5.1. Internet Users (2011)	5,859,118
5.2. Internet Users as Percentage of Population (2011)	70%
5.3. International Internet Bandwidth (bits per second per Internet user) (2011)	27,609
5.4. International Internet Bandwidth (2011) (total gigabits per second [Gbps] per country)	No data
6. Fixed Broadband	
6.1. Fixed Broadband Subscriptions (2011)	1,050,000
6.2. Fixed Broadband Subscriptions as % of Households (2011)	No data
6.3. Fixed Broadband Subscriptions as % of Population (2011)	14.5%
6.4. Fixed Broadband Subscriptions as % of Internet Users (2011)	No data
7. Mobile Broadband	
7.1. Mobile Cellular Subscriptions (2011)	11,727,401
7.2. Active Mobile Broadband Subscriptions per 100 Inhabitants (2011)	58.4
7.3. Number of Active Mobile Broadband Subscriptions (2011)	No data

A Data privacy

The first question in the data privacy section asks if there are laws or regulations governing the collection, use, or other processing of personal information. While there is no specific data protection legislation in the UAE there are several UAE Federal Laws that contain various provisions in relation to privacy and the protection of personal data [16, 17]. Article 31 of the UAE Constitution of 1991 ensures the right of privacy and secrecy of communications; the Civil Transactions Federal Law #5 of 1985 covers liability for unauthorized usage of private information; Articles 378-379 of the Penal Code is concerned with unauthorized use of private information. The Dubai International Finance Center (DIFC), which operates as an independent authority, issued Data Protection Law No.1 of 2007 governing the collection and processing of personal information and disclosure.

The second question examines the scope and coverage of privacy law. The laws are applicable to all seven Emirates of the UAE while the privacy law in Dubai International Finance Center is applicable only within the jurisdiction of the DIFC [17]. Some privacy laws and regulations are sectoral [18]. In the telecommunications sector there are the following laws: Federal Law by Decree No. (3) of 2003 Regarding the Organisation of Telecommunications Sector and Privacy of Consumer Information Policy of 2005.

The third question asks if privacy laws are compatible with the privacy principles in the EU Data Protection Directive. The EU Data Protection Directive is concerned with the protection of individuals with regard to the processing of personal data and with the movement of such data. The DIFC's Data Protection Law #1 is based largely on EU data privacy directives. However, other laws referred to above are not completely in line with those privacy principles [17].

Question 4 looks at whether privacy laws are compatible with the privacy principles in the Asia-Pacific Economic Cooperation (APEC) Privacy Framework. The APEC Privacy Framework offers a set of approaches granting privacy to both individuals and businesses. A study of the UAE's legislation revealed that it is partially compatible with the privacy principles in the APEC Privacy Framework.

The fifth question asks if an independent private right of action is available for breaches of data privacy. According to Practical Law [18] "there is no specific federal data protection law. However, various laws provide for certain privacy rights, the breach of which can give rise to criminal penalties (including imprisonment and/or fines) and/or civil remedies. These laws include the Penal Code, the Cybercrime Law and the Telecommunications Law."

The next two questions ask about an effective agency (or regulator) tasked with the enforcement of privacy laws. There is no specific federal agency or regulator for enforcement of privacy law; however the DIFC has a Data Protection Authority [17].

Question 8 asks if data controllers are free from registration requirements. According to Practical Law [18] "there are no specific provisions under UAE federal law which impose any obligations on data controllers to ensure data is processed properly."

The ninth question asks if cross-border transfers are free from registration requirements. Wugmeister et al. [19] maintain that "the UAE restricts transfers to countries that do not provide adequate protection and require opt-in consent and/or special permits or authorization." No evidence could be found of any recent changes in this regard.

The last question in the data privacy section asks if there is a breach notification law. According to DPL Piper [16] there's no mandatory requirement under UAE Federal Law to report data security breaches.

B. Security

The first question in this section asks if there is a law or regulation that gives electronic signatures clear legal weight. According to Daudpota [20] under Article 17bis(1) of the Federal Law No. 10 of 1992 Concerning Proof in Civil and Commercial Transactions (as amended by Federal Law No. 36 of 2006) "electronic signatures shall have the same force and effect as other signatures mentioned in this law provided they comply with the provisions of the Electronic Transactions & Commerce Law. Further, one can rely on an electronic signature (in place of a physical signature on a document) as long as it is reasonable to do so." Additionally there is a law for the Emirate of Dubai: Law No. 2 of 2002 Concerning Electronic Transactions and Commerce [21]. Under this law an electronic signature is regarded as adequate if a signature is required by law on a document.

Question 2 examines whether ISPs and content service providers are free from mandatory filtering or censoring. Filtering is mandatory and is controlled by the Telecommunication Regulatory Authority [22]. Statistics are published online providing information on blocked content [23]. For example blocked content consists of: material that contradicts with the ethics and morals of the UAE including nudity and dating, material that is not in line with UAE laws, material which expresses hate to religions, material that directly or indirectly constitutes a risk to UAE internet users such as phishing websites and hacking tools, material related to gambling and material related to illegal drugs.

Question 3 looks at whether there are laws or enforceable codes containing general security requirements for digital data hosting and cloud service providers. A report by Cruz [24] maintains that "while the UAE doesn't really have an extensive set of laws, policies, and standards that pertain to the provision of cloud computing services, they have general laws that can be applied in its stead." According to Practical Law [18] "sectoral laws and policies, such as the Cybercrime Law and Privacy of Consumer Information Policy, require service providers to take measures to prevent the unauthorized use or disclosure of personal data."

The next question asks if there are laws or enforceable codes containing specific security audit requirements for digital data hosting and cloud service providers. As no such laws were found it is presumed that none exist. The last question in the section asks about security laws and regulations requiring specific certifications for technology products. Again for this question no laws or regulations were found, but further searching will be conducted.

C. Cybercrime

The first question in this section asks if there are cybercrime laws in place. The UAE issued a federal law on combating cybercrimes in 2006. Cyber-Crime Law No. 2 of 2006 considers any intentional act that abolishes, destroys, or reveals secrets, or that results in the republishing of personal or official information to be a crime" [25]. In 2012 the UAE issued a far more comprehensive cybercrime law: Federal Decree-Law no (5) of 2012 on Combating the Cyber-Crime [25].

The second question examines whether cybercrime laws are consistent with the Budapest Convention on Cybercrime. The Budapest Convention on Cybercrime is an international treaty that seeks to address Internet and computer crime by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations. A study of UAE cybercrime law by Talal [26] shows that there is partial compliance with the Budapest Convention. The law is vague in places using terms that are not clear and not providing information on penalties. For example the law does not clarify the penalty of constructing terrorist websites or spreading terrorist information online [26].

The next question looks at what access law enforcement authorities have to encrypted data held or transmitted by data hosting providers, carriers, or other service providers. According to Practical Law [18] "criminal sanctions can be enforced against an offender by the police for violation of the Penal Code or the Cybercrime Law, and prosecuted by the public prosecutor in the criminal courts."

Question 4 examines how the law deals with extraterritorial offenses. Khasawneh and Ahern [25] state that "offences under the law may be treated as criminal and therefore will have extra-territorial effect. A crime can be considered to have occurred within the UAE if any of its constituent acts occur in the UAE, or if the result of the acts has been, or is intended to have been, in the UAE."

D. Intellectual Property Rights

The first question in this section asks if the country is a member of the TRIPS Agreement. The Agreement on Trade-Related aspects of Intellectual Property Rights (TRIPS) is an international agreement administered by the World Trade Organization (WTO) that specifies minimum standards for many forms of intellectual property. According to Sunil Thacker Associates [27] "the country is a member of the TRIPS Agreement since April 1996." Question 2 looks at whether IP laws have been enacted to implement TRIPS. Sunil Thacker Associates [27] maintain that "Federal Law No. 17 of 2002 repealed the Patent Law No. 44 of 1992 to bring UAE legislation into line with the TRIPS agreement."

The next question asks if the country is party to the WIPO Copyright Treaty. The World Intellectual Property Organization (WIPO) Copyright Treaty is an international treaty on copyright law. The UAE is a member of WIPO Copyright Treaty since 2004 [28].

Question 4 asks if laws implementing the WIPO Copyright Treaty have been enacted. According to WIPO there are 23 laws and regulation and 36 treaty memberships in this regard in the UAE [28].

The next question examines if civil sanctions are available for the unauthorized making available (posting) of copyright holders' works on the Internet**.** A report by UNESCO [29] says that in the UAE "legal action may be instituted at the request of the author, the copyright holder or their successors, including fair and equitable civil judicial procedures under Articles 34 and 35 of the Law on Copyrights and Neighboring Rights."

The sixth question is similar to the previous question but asks about criminal rather than civil sanctions. According to Sunil Thacker Associates [27] "unauthorized publication of an author's work constitutes a criminal offence and penalizes the offender with a fine."

Question 7 examines whether there are laws governing ISP liability for content that infringes copyright. The International Intellectual Property Alliance in its Special Report on Copyright Protection and Enforcement [30] states that "the cybercrime law was recently updated to include, among other things, a specific provision on ISP liability. However, the law does not cover ISP liability in connection with IP infringement."

The next question asks if there a basis for ISPs to be held liable for content that infringes copyright found on their sites or systems. The answer is based on the statement by the International Intellectual Property Alliance [30] statement given in the above question.

The ninth question concerns what sanctions are available for ISP liability for copyright infringing content found on their site or system. As the law does not cover ISP liability in connection with IP infringement then this question is not applicable.

Question 10 looks at whether ISPs must take down content that infringes copyright, upon notification by the copyright holder. According to the International Intellectual Property Alliance [30] there are no specific guidelines on ISP liability for infringed copyrights as stated above, but ISPs, they say, are cooperative when it comes to removing unauthorized content.

The next question asks if ISPs are required to inform subscribers upon receiving a notification that the subscriber is using the ISP's service to distribute content that infringes copyright. The answer is no because, as stated above, there are no specific guidelines on ISP liability for infringed copyrights.

The last question examines if there is clear legal protection against misappropriation of cloud computing services, including effective enforcement**.** There is only limited protection as there are no clear copyright protection measures to hold providers liable for infringement [30].

E. Support for Industry-led Standards & International Harmonization of Rules

The first question in this section asks if there are there laws, regulations or policies that establish a standards-setting framework for interoperability and portability of data. None could be found so the answer presumably is no. However further searching will be conducted.

Question 2 asks if there is there a regulatory body responsible for standards development for the country. There is a regulatory body known as the Emirates Authority for Standardization & Metrology (ESMA) which was established in 2001 (see www.esma.gov.ae).

The next question asks if e-commerce laws are in place. A federal law known as Federal Law No. (1) of 2006 on Electronic Commerce and Transactions was established in 2006 [31].

Question 4 asks what international instruments the e-commerce laws are based on. According to the United Nations Commission of International Trade Law (UNCITRAL) legislation based on their 1996 Model Law on E-Commerce was established in the UAE in 2006 [32].

The fifth question asks if the downloading of applications or digital data from foreign cloud service providers is free from tariffs or other trade barriers. The answer is yes as according to the Office of the United States Trade Representative the list of tariffs applied by UAE doesn't include downloading of data from cloud service providers [33].

Question 6 asks if international standards are favored over domestic standards**.** No information was found on this but further research is continuing.

The last question in this section examines whether the government participates in the international standards-setting process. The UAE standards-setting institution, the Emirates Authority for Standardization & Metrology (ESMA), adopts international standards and participates in the following international organizations: International Organization for Standardization (ISO); The Codex Alimentarius Commission (Codex); International Electrotechnical Commission (IEC); International Laboratory Accreditation Cooperation (ILAC); Arab Industrial Development and Mining Organization (AIDMO); Standardization Organization for GCC (GSO) [34].

F. Promoting Free Trade

The first question in this section asks if there are any laws or policies in place that implement technology neutrality in government. No laws or policies were found in regard to this so it is presumed that none are in place.

Question 2 asks if cloud computing services are able to operate free from laws or policies that mandate the use of certain products (including, but not limited to, types of software), services, standards, or technologies. According to Yates [35] "the UAE does not have a comprehensive set of laws, regulations and/or official standards specifically for the provision of cloud computing services, and general laws apply."

The next question asks if cloud computing services are able to operate free from laws or policies that establish preferences for certain products (including, but not limited to, types of software), services, standards, or technologies. As stated in the answer to the previous question there are no laws or regulations or official policies in relation to cloud services so providers can operate freely in that regard.

The last question in this section asks if cloud computing services able to operate free from laws that discriminate based on the nationality of the vendor, developer, or service provider. The answer to this again is yes because as said in the previous two responses there are no laws, regulations or official policies for cloud providers.

Table 3. Scores in each category for all countries

Rank	Country	Total	Data Privacy	Security	Cybercrime	Intellectual Property Rights	Support for Industry-Led Standards & International Harmonization of Rules	Promoting Free Trade	ICT Readiness, Broadband Deployment
1	Japan	84.1	8.8	8.4	10	17.2	8.8	9.2	21.7
2	Australia	79.9	7.9	6.4	10	17.6	10	7	21
3	United State	79.7	6.5	7.6	8.8	16.6	10	8	22.2
4	Germany	79.1	6.6	6.4	10	16.8	9.8	9.2	20.3
5	Singapore	78.5	7.6	3.6	9	18	8.8	8.6	22.9
6	France	78.3	6.5	7.6	10	16.8	9.6	8.8	19
7	United Kingdom	76.9	6.9	8	6.8	17.8	9.2	6.8	21.4
8	Korea	76.2	9.3	6	4.8	17.6	9.6	7	21.9
9	Canada	75.8	8.1	6.8	6.2	15.6	10	9.6	19.5

10	Italy	75.5	6.2	7.6	9.6	17	9.8	8.8	16.5
11	Spain	73.7	6.5	6.4	8.8	15.2	9.8	9.4	17.6
12	Poland	72	6.8	5.6	8.8	16.8	9.8	8.4	15.8
1	Malaysia	69.5	7.1	5.6	7.2	17.4	10	5.8	16.4
14	**UAE**	**69.3**	**6.5**	**4**	**8.5**	**16**	**6**	**8**	**20.3**
15	Russia	59.1	5.4	5.6	6.8	14.4	6.8	5.2	14.9
16	Mexico	56.9	7.5	4.8	8.6	12.4	9.2	3	11.4
17	Argentina	56.5	5	6	8.8	12.4	4.6	5.8	13.9
18	India	53.1	4.1	4.4	7.4	12	10	6.4	8.8
19	Turkey	52.4	3.5	4	6.4	14	8.6	2.8	13.1
20	China	51.5	4.7	2.8	4.6	13.6	7.8	4.8	13.2
21	South Africa	51.3	2.8	3.2	9.8	13.6	9.8	1.8	10.3
22	Indonesia	48.4	6.4	3.2	7	11.2	8.2	2	10.4
23	Brazil	44.1	4.7	3.6	8	8.8	3.4	2.2	13.4
24	Thailand	44	3.5	1.6	7.4	8	8.8	3	11.7
25	Vietnam	40.1	4.1	2.8	5	9.2	7	1.4	10.6

IV. Discussion

The scores for the UAE for each of the seven categories is shown in Table 3. Scores are also shown for the other 24 countries for comparative purposes. The UAE achieved an overall score of 69.25 which placed it in position 14.

Comparing UAE to other countries, it may be seen that the country has developed effective strategies for cybercrime and intellectual property rights protection. In these two categories the UAE achieved nearly as high a score as highly ranked countries such as Canada, Australia, Singapore, and Japan. In the category of free trade the UAE did very well again achieving a score similar to the top ranked countries showing that the policies for promoting free trade are among the best worldwide. For ICT readiness and broadband deployment the UAE did very well achieving a score of 20.3 which is not far behind the top scoring countries of Singapore (22.9) and the United States (22.2). However data privacy and security are major concerns for potential individual and organizational cloud computing users in UAE. The scores in both these categories are low and place the UAE in the bottom one third of the countries. This result is corroborated by a study by Danaher & Chong [9] in 2014 of user perceptions of privacy in the UAE. That study showed that users in the UAE believe that cloud computing is intrinsically insecure and they felt that they could not trust cloud providers to keep their data secure and private.

V. Conclusion

Overall the results show that the UAE has a relatively good level of "cloud computing readiness". In comparison with a range of other countries from Japan, a well-developed nation, to Vietnam, a developing nation, it sits around the midway mark. It has progressive strategies in place aimed at ICT capacity raising, free trade support, international standards support and integration, intellectual property protection and cybercrime. However more attention needs to be paid to policies to improve data privacy and security.

References

[1] L.Vaquero and L.Roderp-Merino, "A break in the clouds: towards a cloud definition". *ACM SIGCOMM Computer Communications Review, 39*(1), 2009, pp. 50-55.

[2] A. Weber, "Cloud computing in education in the Middle East and North Africa (MENA) region: can barriers be overcome?" The 7th International Scientific Conference eLearning and Software for Education, Bucharest. 2011

[3] A. Seth, H. Agrawal and A. Singla, Integrating SOA and Cloud Computing for SME Business Objective, WSEAS Transactions on Computers, Issue 3, Volume 11, 2012, pp.77-87

[4] J. Gantz, S. Minton and A. Toncheva, "Cloud computing's role in job creation", IDC, 2012, Available: http://news.microsoft.com/download/features/2012/IDC_Cloud_jobs_White_Paper.pdf

[5] 2013 BSA global cloud computing scorecard. BSA-The Software Alliance, 2013. Available: http://cloudscorecard.bsa.org/2013/assets/PDFs/BSA_GlobalCloudScorecard2013.pdf

[6] State of cloud computing in the UAE. Frost & Sullivan, 2013. Available: http://www.reportlinker.com/p01628615/State-of-Cloud-Computing-Security-in-the-UAE.html

[7] W. Chen, "Cloud computing in UAE context: An institutional perspective". Proceedings of International Conference On Information Resources Management, 2011 Available: http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1004&context=confirm2011.

[8] B. Byrne, "Cloud computing: what you should and shouldn't be worried about", MeshIP, 2011 Available: http://meship.com/Blog/2011/02/04.

[9] K. Hashizume, D.Rosado, E. Fernández-Medina, E. Fernandez, "An analysis of security issues for cloud computing". *Journal of Internet Services and Applications,* 2013. Available: http://link.springer.com/article/10.1186/1869-0238-4-5

[10] G Sharma, S. Bevinakoppa, S. Venkatraman, Modeling of Secured Cloud Network - The Case of an Educational Institute, Recent Researches in Information Science and Applications, Eds: A Corbi, J. Metrolho, A. Lysko and R. Furgeri, WSEAS Press, 2013, pp. 150–155
[11] A. Prangishvili, O. Shonia, I. Rodonaia and V Rodonaia, Recent advances in automatic control, information and communications, Eds: A. Zak and A. Slaby, WSEAS Press, 2013
[12] M. Danaher and C. Chong, "User concerns on cloud security – a UAE perspective", International Journal of Computer and Information Technology, Vol 3(6), 2014, pp 1264 - 1269
[13] S. McBride, UAE cyber security authority unveils policies, standards. ITP.net. 2014, Available: http://www.itp.net/598777-uae-cyber-security-authority-unveils-policies-standards.
[14] R. Berry and M. Reisman, "Policy challenges of cross-border cloud computing". *Journal of International Commerce and Economics.* 2012, Available: http://www.usitc.gov/journals/Policy_Challenges_of_Cross-border_Cloud_Computing_rev.pdf.
[15] UAE rankings, Telecommunication Regulatory Authority, 2014. Available: http://www.tra.gov.ae/UAE_rankings.php
[16] Data Protection Laws of the World, DPL Piper, 2014, Retrieved from http://dlapiperdataprotection.com/#handbook/law-section/c1_AE2
[17] 2014 International Compendium of Data Privacy Laws, BackerHostetlerm 2014. Retrieved from: http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/International-Compendium-of-Data-Privacy-Laws.pdf
[18] Data protection in United Arab Emirates: overview, Practical Law, 2014. Retrieved from: http://uk.practicallaw.com/0-518-8836#a487999.
[19] M. Wugmeister, K. Retzer, C. Rich. Global Solution for Cross-Border Data Transfers: Making the Case for Corporate Privacy Rules, Georgetown journal of international law, Vol 38, pp 449-498, 2007, Retrieved from http://media.mofo.com/docs/pdf/0801CrossBorder.PDF
[20] F. Daudpota, United Arab Emirates: Reliance on Electronic Signatures and Secure Electronic Signatures under the UAE Law, Mondaq, 2010, Retrieved from: http://www.mondaq.com/x/105452/IT+internet/Reliance+on+Electronic+Signatures+and+Secure+Electronic+Signatures+under+the+UAE+Law.
[21] Law No. 2 of 2002 of the Emirate of Dubai – Electronic Transactions and Commerce Law 2002, Retrieved from http://www.dubai-law.org/
[22] Internet filtering in the United Arab Emirates, OpenNet Initiative, 2009, Retrieved from: https://opennet.net/research/profiles/uae.
[23] Internet Access Management (IAM) Statistics, Telecommunication Regulatory Authority, 2014, Retrieved from: http://www.tra.ae/IAM_Statistics.php
[24] X. Cruz, The State of Cloud Computing Around the World: United Arab Emirates, Cloud Times, 2013, Retrieved from: http://cloudtimes.org/2013/04/01/the-state-of-cloud-computing-around-the-world-united-arab-emirates/.
[25] N. Khasawneh and G.Ahern, Cyber Crimes Law - United Arab Emirates. Eversheds, 2012, Retrieved from: http://www.eversheds.com/global/en/what/articles/index.page?ArticleID=en/Technology/TMT_tech_cyber_crimes_law_uae_dec12.
[26] I. Talal, SWOT Analysis: U.A.E. Cyber Law. Zayed University, 2012, Retrieved from: https://www.academia.edu/386865/SWOT_Analysis_U.A.E_Cyber_Law.
[27] Intellectual Property Guide: United Arab Emirates. Sunil Thacker Associates, 2014. Retrieved from: http://www.ama.ae/UAE-Intellectual-Property-Law.pdf
[28] United Arab Emirates: IP Laws and Treaties. WIPO, 2013. Retrieved from: http://www.wipo.int/wipolex/en/profile.jsp?code=AE.
[29] United Arab Emirates: Country profile based on information provided by regional experts, UNESCO World Anti Piracy Observatory, 2009. Retrieved from: http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CLT/diversity/pdf/WAPO/uae_cp_en.pdf
[30] 2014 special 301 report on copyright protection and enforcement, International Intellectual Property Alliance, 2014, Retrieved from http://www.iipa.com/2014_SPEC301_TOC.htm
[31] Federal Law No. 1 of 2006 on Electronic Commerce and Transactions, Telecommunication Regulatory Authority, n.d., Retrieved from: http://www.tra.ae/pdf/legal_references/Electronic%20Transactions%20%20Commerce%20Law_Final%20for%20May%203%202007.pdf
[32] UNCITRAL Model Law on Electronic Commerce, United Nations Commission on International Trade Law, n.d., Retrieved from: http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model_status.html.
[33] National Trade Estimate Report on Foreign Trade Barriers: UAE. Office of the United States Trade Representative, 2014, Retrieved from: http://www.ustr.gov/sites/default/files/United%20Arab%20Emirates.pdf.
[34] B. Tarawneh, Standards & Support of the Retail / National Industry. ESMA, n.d., Retrieved from: http://www.sialme.com/getattachment/Conference---Workshops/Conference/Mr-Basem-Hamad-Al-Tarawneh.pdf.aspx.
[35] D. Yates, Cloud computing in the UAE: Legal risks and remedies for providers and users. Al Tamimi & Co., 2011. Retrieved from: http://www.tamimi.com/en/magazine/law-update/section-7/june-5/cloud-computing-in-the-uae-legal-risks-and-remedies-for-providers-and-users.html#sthash.V2QfonC1.dpuf.

Maurice Danaher is an Associate Professor in the College of Technological Innovation at Zayed University, Abu Dhabi. He received his PhD in Computing and Information Systems from Swinburne University of Technology, Melbourne, Australia, in 2003. He received his Bachelor and Masters degrees in Engineering from the National University of Ireland, Cork, Ireland. His research is the areas of Information Technology and Education. In IT he has published on cloud computing, artificial intelligence, graph layout and computer graphics. In Education he has published on quality measurement.

Saif Al Rumaithy has been a postgraduate student in the College of Technological Innovation at Zayed University, Abu Dhabi. He received his M.Sc in IT in 2014 from Zayed University.