Journal of Theoretical and Applied Information Technology
20th June 2016. Vol.88. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

SECURITY, PRIVACY, ACCESSIBILITY AND AVAILABILITY ISSUES ADDRESSED WHEN DEVELOPING WEBSTIES IN THE GCC

[1,2]DIMITRIOS XANTHIDIS, [3]GEORGE VIOLETTAS,
[1]Dhofar university, Department of Management Information Systems,
College of Commerce and Business Administration, Oman
[2]CIBER-Research.eu UK
[3]Technical Trainers College, Saudi Arabia
E-mail: [1]dxanthidis@du.edu.om, [3]georgevio@gmail.com

ABSTRACT

This study on the evaluation of the Web sites of companies in the GCC (Gulf Council Countries) and attempts to answer the question of whether security and privacy but, also, accessibility and availability issues are addressed by the developers locally. A total number of 129 web sites from companies in Bahrain, Kuwait, Saudi Arabia, Qatar and United Arab Emirates were evaluated based on the WSEI (Web Site Evaluation Index) were applied during the evaluation. The results of the evaluation are not encouraging at all showing that security and privacy issues are not a priority when developing the web sites and accessibility and availability are not among their serious concern either.

Keywords: *Websites, Evaluation, Security, Privacy, Accessibility, Availability, GCC*

1. INTRODUCTION

The modern business is operating in a digital online environment regardless of the particularities of the sector it belongs to. This brings many opportunities to attract potential clients but, also, demands careful and thorough strategic planning of how certain challenges are to be addressed.

During the past decade, or so, the executives in the GCC have been active in responding to the growing number of people using the Internet. Currently 15% of the businesses in the Middle East and GCC have an online presence with the GCC companies in the lead [1]. At the same time the younger individuals, aging below 40 and being very active in the social networks [2], are being targeted by the marketing officials of these companies. Furthermore, the higher education institutions intensify their efforts in training local individuals on the new web technologies in an effort to prepare the manpower for the next decade web-designers in the region.

The task of designing an effective web site becomes increasingly critical in importance and large in size when the objective is not just to have an online presence but, moreover, to deploy additional everyday operations on the Web as the Website Evaluation Index (WSEI) suggests [3]. No doubt, among the most important issues to be addressed in this process are those related to security of the websites and the privacy of the online clients in addition to ensuring availability of the online presence on a 24/7 basis and its full compatibility with different electronic devices and platforms.

The question this paper is attempting to answer is to what extend these regional companies with online presence are successful in deploying web solutions that address the aforementioned issues.

2. BACKGROUND

2.1 Security on the Web

Although many researchers acknowledge that Websites are running in a largely insecure web browser environment [4] and some even suggest security policies with strict rules of read/write for every system component [5], most studies on metrics for websites do not consider security as one of the aspects of web site design. In [6] the authors clearly state that "… a usability evaluation of secure software should not focus

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

on usability to exclusion of security …". In [7] there is a framework for web metrics, i.e. usefulness, ease of use, enjoyment, content & design, where security cannot fit in any of these existing categories. One could argue that placing security below Design and/or Content is obviously giving the wrong impression to users and designers.

Other authors claim that, although the input validation is important but it is never perfect, looking for other solutions like validating the origin of the call from "trusted" and untrusted "sources"/websites [4] to define security policies. In [8], a good, i.e. appealing for visitors, website in terms of usability, amount and quality of informative content, customer service and web security, shall be perceived as a superior (in quality) website. Hence, a quality website is described as the one which provides ease of use and effectiveness of the purchase mechanisms, trust, user satisfaction and perceived lower transaction risk. Security is also directly connected to loyalty [9]. In other words, if a user feels that the website is offering high levels of security, s/he will visit it repeatedly n the future.

It is also very important not to focus only on the attackers' actions and intentions when considering the security of a website but, also, on the ordinary users' attempts for security breach, either because of misunderstanding or lack of information, or simply because of not knowing/understanding certain actions are causing such problems [10]. In [6], in addition to the above, the authors conduct a usability/security audit of websites by utilizing usage scenarios and comparing results.

Having said that, it is necessary and indeed very helpful to identify the possible attacks that constitute potential vulnerabilities of the web solutions. Such lists are formed more than a decade now and include various forms of attacks including injections among which the most important and frequent, as it seems, are XSS and SQLi. In the case of XSS (Cross Site Scripting) the attackers insert malicious code into websites viewed by the victims and causing the extraction of personal and confidential information (e.g. credit card info) stored in the web server of the company related to its customers [11]. OWASP has released a cheat sheet (a roadmap) for coders in order to eliminate XSS from a website [12]. Although the idea sounds very good, in practice it is very difficult to follow those exact guidelines without missing even one entry point that is enough for a possible attack. In the case of SQL injection (SQLi) malicious code is inserted into an entry point of a website, e.g. through forms asking user data and receiving such data as SQL commands, and yields a lot of data that possibly should be locked and protected as confidential for the companies. This form of vulnerability has declined by 7% in 2012 as a study has shown [13]. This same study revealed 53% of the organization had a central application library or framework enforcing security policy and 23% of the organizations said that they had a data/system breach due to application layer vulnerability.

In general, the way to stop injection attacks is already known and standard: every input has to be sanitized, automatically as some researchers suggest (e.g. [14, 11]) or by better coding. The main idea behind this is that a unique central sanitization method should be used [15], very well tested and documented. Under no circumstances this method should be created "in house" but rather use one well known and tested (avoid reinventing the wheel), since a lot of web frameworks provide sanitization of input [16, 17].

2.2 Privacy on the Web

One of the most interesting facts about Internet users' privacy is that while most of them admit they are very concerned about their privacy but they neglect to take measures to protect it. On the other hand, the website owners many times do warn about this issue but this remains invisible or remote for the end-user [18]. Users on the web have three major privacy concerns: (1) information transfer, (2) notice/awareness, and (3) information storage [19]. Consequently all privacy notices should address the above. The collection of IP addresses and other similar browsing behavior data should be clearly advertised on the website and the users should be asked for their consent.

In another study, although 63% of the users agreed with a statement of consent for third parties monitoring activities [20], such a statement should exist in order for someone to consent to it. The same study suggests that only half of the users agreed with a consent for revealing user's location and only a little over 50% agreed to consent about inference of demographic information, with female users more than male.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The need for privacy has led to privacy seals, which are, simply put, reassurances from a respectable institute that one's personal and/or sensitive data is treated with respect and confidentiality. Privacy seals and the content of privacy policies can be viewed as somewhat convincing efforts of the website owners to reduce the customers' feeling of risk of abuse of personal information [21]. The most important value of such statements is that, most of the times, they are the only relevant information a user can get from a website. In [22] only 6% (out of 64 such policies examined) were accessible and reasonably clear to understand to the 28% of the population with high school education whereas 54% were beyond the grasp of 56% of the Internet users since they required more than 14 years of formal education and another 13% of them required Internet users with an M.Sc. degree in order to understand them! It is only reasonable to assume, if that is the case, that a very large portion of Internet users can only understand a very limited part of those policies. On the bright side, as another study suggested, people will have fewer privacy concerns for websites they trust but still they don't want their data to be collected implicitly [23] perhaps because they feel this violates their trust to these organizations/companies.

Finally, it is also rather interesting to observe how privacy-relevant laws affect advertising for the Internet and the Web. In the case of E.U., for example, the newly passed (stricter) laws posed a lot of restrictions on personal data sharing that caused the effects of advertising to drop by up to 65% when compared with the rest of the world. The oxymoron is, in this case, that users are protecting their personal data but the advertisements they get while browsing are almost completely irrelevant to their persona and interests and, hence, annoying and useless, not to mention sometimes offensive, e.g. when religious symbols are used to, accidentally, address different religion followers [24]. A recent study [18] indicated the little resistance to purchasing online common goods, e.g. batteries, but when it came to more personal value or items, e.g. books, etc., they showed increasing levels of hesitation. A decisive factor on purchasing those "personality revealing" items was whether offered under a higher level of privacy. People were likely to pay a premium for this privacy assurance.

2.3 Accessibility and availability on the Web

Availability is determined as the time that the website is "up and running". The website also has to be available to the users, with all its functionalities or extra features, e.g. the connection/redirection to PayPal or similar organizations for secure purchases online, in a "meaningful" amount of time which was set long ago to be up to 2'' [25]. The same study suggests the logical conclusion that users are not tolerant to delays and they lose patience easily. On the other hand, websites that are "fast" let the user make more navigation errors and search. Therefore, apparently, availability is strongly connected to loyalty of users. Also the better the navigability of the website the greater the customer loyalty it attracts [9, 26]. In other words, a user is not visiting a website repeatedly unless that person can find what s/he is looking for rather quickly.

More than 83% of web users will leave a website if they get the feeling of too much complexity on finding a product or service and 58% of those who experienced usability issues never return to this website. In about 60% of the time people didn't find what they were looking for in a website and it can be reasonably assumed that they abandoned it and never returned back [8]. Surveys suggest that even the search behavior of users is highly altered depending on delays. Users did not go in much depth and examined fewer documents on the matter when the search results were delivered to them with delay [27].

Similar effects can be assumed if websites are not accessible through a variety of electronic devices including, most likely, smartphones, tablets, etc.

3. OBJECTIVES AND METHODS

The main idea behind this study is to evaluate the websites of companies in the GCC. More specifically the following objectives were targeted:

- Examine whether necessary development strategy is followed to ensure security and privacy issues are addressed,
- Verify, if possible, the availability and accessibility of the websites under different operating platform and on a variety of current electronic devices.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3.1 Website Evaluation Index (WSEI)

The WSEI [3] provides a list of useful suggestions of what are the functional and non-functional requirements a website of any online company in any region of the globe should address. It is divided into 4 distinct categories. The first two, i.e. HCI (human-computer interaction) related issues called "stickiness" and guidelines associated with customization and/or globalization needs were covered in [28]. This paper covers the other two categories, namely accessibility and availability requirements and assessment of whether proper security and privacy are measures implemented for the web solutions.

3.2 Evaluation scope

The WSEI together with the aforementioned tests provides a clear list of security and privacy but, also, accessibility and availability issues that should be addressed by the web solution developers although more could be included in it. They are divided into two broad categories.

The 1st category includes issues related to security and privacy provisions taken when developing the website:

- Does it provide secure login?
- Does it provide transactions through a secure channel?
- Doe it use TLS instead of the old SSL or even no secure channel?
- Is there a certificate verifying the channel?
- What is the security key size?
- Does it make any anti-virus scanner available to the users?
- Does the website time-out to ensure secure transactions?
- Is it vulnerable to Denial of Service (DoS) attacks?
- Does it ask for the users' consent when using tracking mechanisms?
- Does it include a privacy statement?
- Are the email addresses masked for security and/or privacy reasons?

The 2nd category includes issues related to the accessibility and/ or availability characteristics of a website:

- Is it compatible across different platforms, i.e. especially with current electronic devices like tablets, smartphones, etc.?
- Is it optimized for the handicapped or people with disabilities?
- Is it loading in a reasonable time?
- Is it displayed properly at different resolutions?
- Does it support "third party" components, i.e. does it offer downloadable components from other companies?

3.3 The sample

This is the 2nd part of the evaluation of the websites of the companies in the GCC countries, namely Bahrain, Kuwait, Saudi Arabia, Qatar, and United Arab Emirates. Like in the 1st part, it examines the level of quality of the websites of 129 companies conveniently selected from each country and in particular 7 from Bahrain, 12 from Kuwait, 78 from Saudi Arabia, 4 from Qatar, and 28 from U.A.E. These countries from the region were selected as been more technologically and financial advanced with high Internet penetration and an increased level of computer and Internet literacy as opposed to others in the region under study.

The difference with this part is the context of the questions answered which now address security and privacy issues, instead of human-computer interaction and customization/globalization issues in the 1st part but, also, with the provisions of the web developers associated with the accessibility and availability of the websites under different platforms and on a variety of electronic devices.

In all the above questions/issues a negative answer would result in a 0 whereas a positive one would be valued with 1. All these data once recorded were processes through SPSS for cross-tabulation and ANOVA statistical analysis and the results transferred to MS Excel for the production of charts.

4. FINDINGS

4.1 Results at a glance

In general, it could be said that the findings are not satisfactory indicating very poor development strategies followed in all the aforementioned categories. Figure 1 illustrates these findings in some detail.

In the case of security the online strategies do not address but in very limited way and only in limited cases the major issues. Furthermore, in general, the websites seem to be vulnerable to cross-scripting and denial-of-service attacks. Concerning the privacy of the online visitors it seems that half of the companies follow some

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

provisions somewhat successful whereas the other half just don't. Finally, as to the accessibility and availability issues addressed, with the exception of ensuring that the websites are displayed properly in different platforms, the rest are simply just ignored.

The above support the claim that most of the websites evaluated look old and "abandoned". They look as if there was no planning followed but, rather, a somewhat ad hoc and "quick and dirty" approach of just developing a website for the, perceived as, basic needs of the companies.

4.2 Security features

Figures 2 and 3 depict and table 1 details the results of the evaluation of the 128 websites. The results reveal a number of serious problems concerning their secure connections (https) and, also, some others when addressing (actually not) privacy and related issues.

The results as to secure login provisions are very poor (aggregate mean: 0.23/1). The only exception would be the case of Qatar but only as an indication since the sample was very small, i.e. only 7 websites evaluated. Secure channels are not very much used either and, when they are, the SSL protocol version 1.5 is used (which has security issues) instead of the latest TLS. To make things worse, even the key used is only 128 bit (0.13) although the trend in the developed countries is to easily have 256 or 512 bit encryption without a significant compromise in the communication speed (figure 3). Add to the above that there are websites with expired SSL certificates or certificates not issued by a trusted certificate agency (0.28). Even if this, for some, is not considered a severe problem, however, it sends a negative sign for the reputation of the company represented by the website.

Most of those websites using SSL for the final transaction (0.29) are not utilizing it for the user login page! This is a major security breach because someone can easily intercept the user credentials having access to the user account. In the case of the websites where all information exchange pages are encrypted the answer to the question if secure channel (TLS or other) was used for economic transaction was based on evidence declared on the website. (If the username & password were sent over unsecure channel there was no clear and safe way to check the transactions protocol).

The number of websites with obvious signs of cross-scripting (XSS) flaws is rather high (0.256). This is one of the easiest attacks to deploy. Also some websites show profound signs of vulnerability against SQL injections (SQLi). For the economy of time and to avoid possible legal complications the vulnerabilities were not explored any further. It should be noted that, most likely, many of the websites were developed using Joomla. This gives some basic security features such as (at least at the basic level) protection against XSS and DoS (Denial of Service attacks).

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

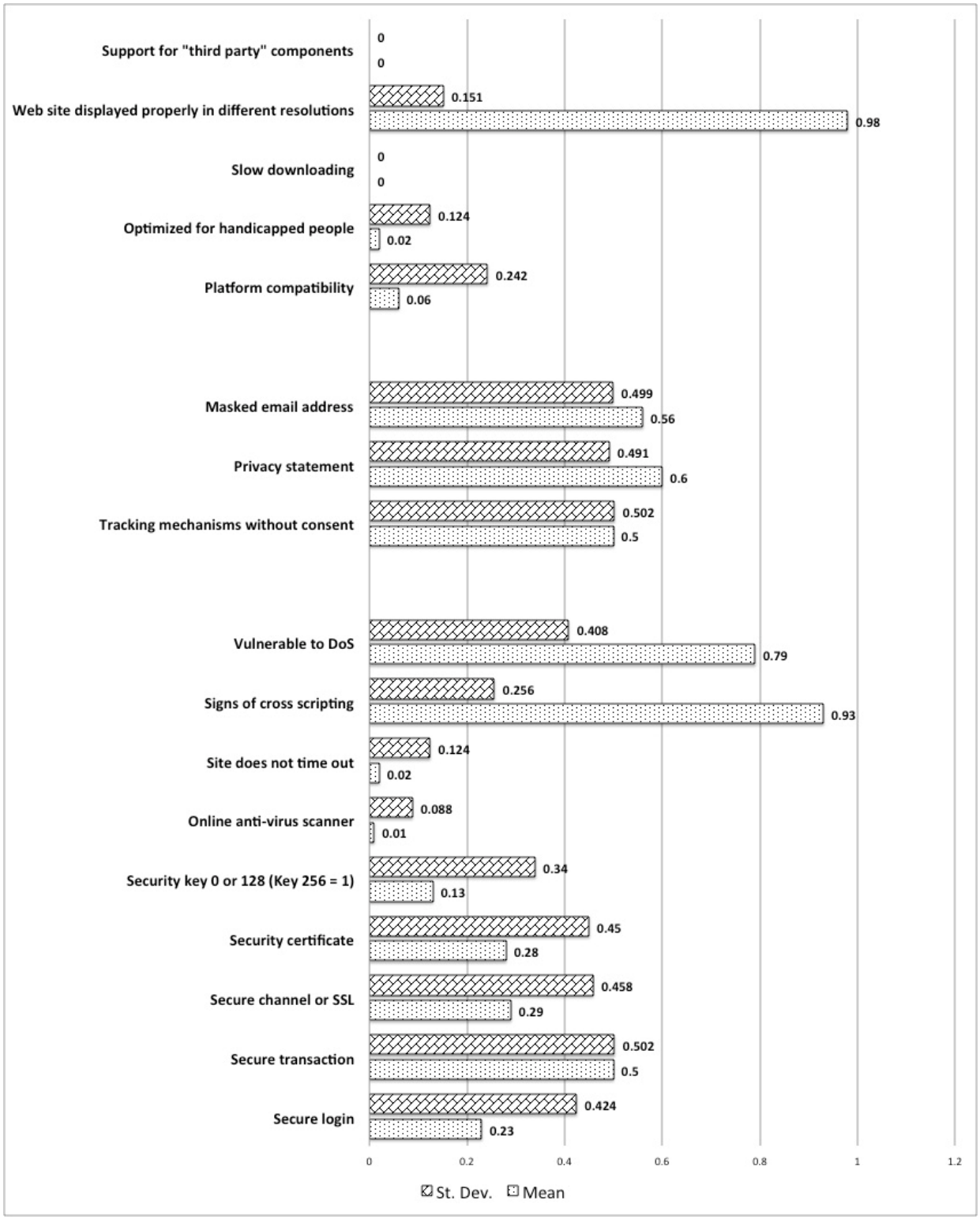

Figure 1 Results at a Glance

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

On the other hand, since https is not by default enabled in Joomla as to username & password exchange, almost all of the websites lack this feature, making them completely vulnerable as to leak of personal information of the users. This simply means the developers used something "out of the box", put the site "in the wild" and just forgot about it. Nowadays, maintaining strong security requires constant monitoring, continuous updates, personal effort and above all total awareness.

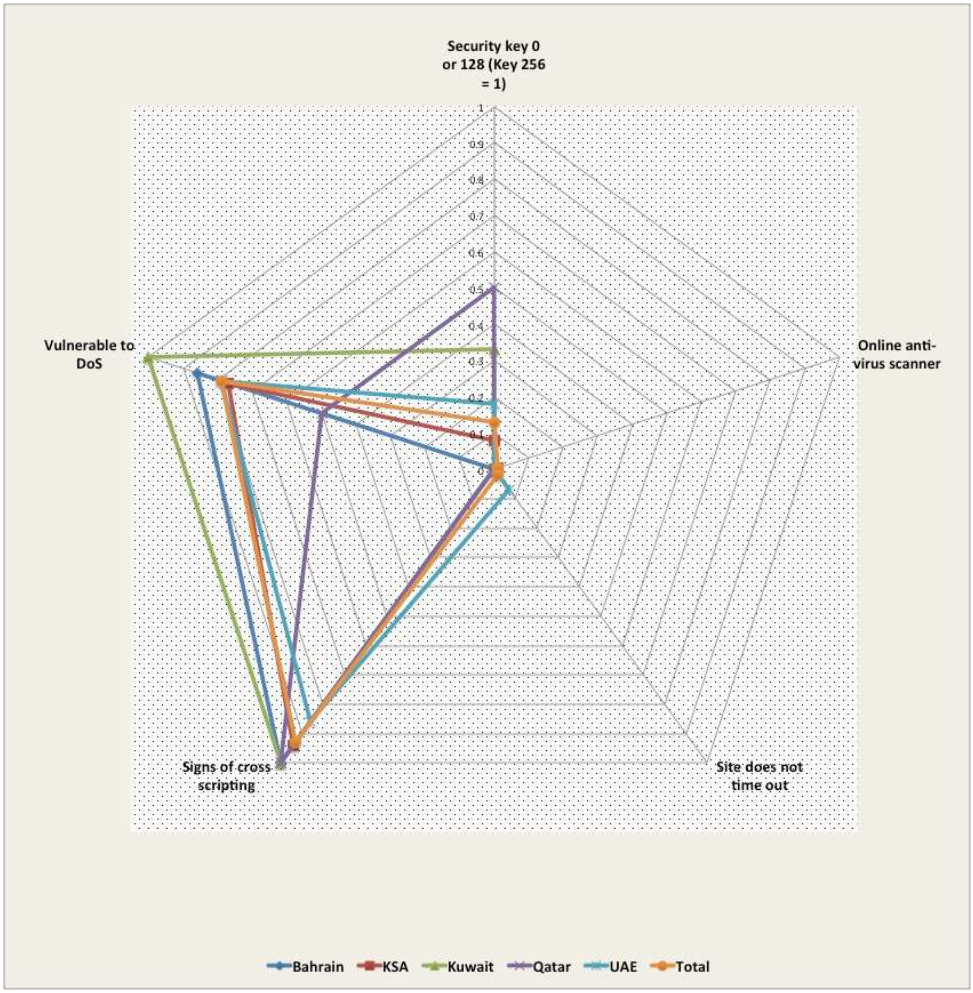

Figure 2. Security Features Implemented (Part I)

Journal of Theoretical and Applied Information Technology
20th June 2016. Vol.88. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

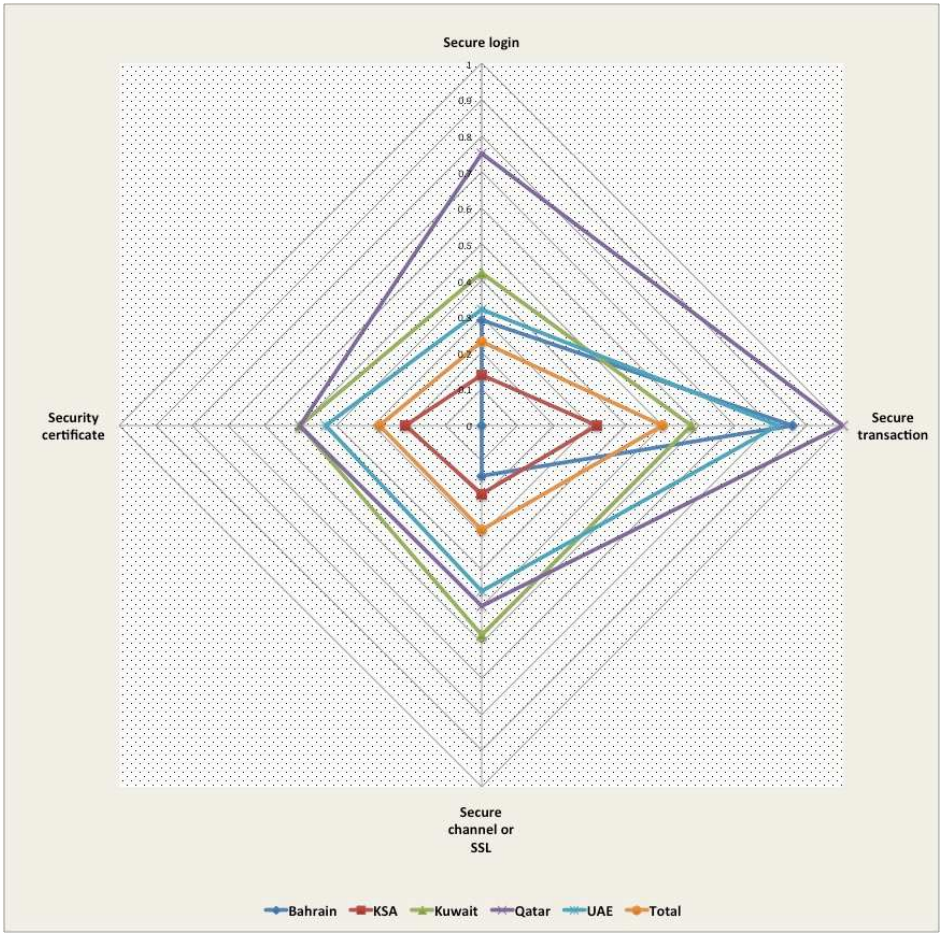

Figure 3. Security Features Implemented (Part II)

Table 1. Security features implemented (Mean: 0 = Negative, 1 = Positive)

	Secure login	Secure transaction	No channel or SSL	Security certificate	Security key (0 or 128 = 0, 256 = 1)	Anti-virus scanner	Site time-out	Sings of XSS	Vulnerable to DoS	N
GCC	0.23	0.29	0.29	0.28	0.13	0.01	0.02	0.256	0.79	**129**
Bahrain	0.29	0.86	0.14	0.0	0.0	0.0	0.0	1.0	0.86	**7**
Saudi Arabia	0.14	0.32	0.19	0.21	0.08	0.01	0.0	0.94	0.77	**78**
Kuwait	0.42	0.58	0.58	0.5	0.33	0.0	0.0	1.0	1.0	**12**
Qatar	0.75	0.5	0.5	0.5	0.5	0.0	0.0	1.0	0.5	**4**
U.A.E.	0.32	0.46	0.46	0.43	0.18	0.0	0.07	0.86	0.79	**28**

Table 2. Accessibility, availability and privacy provisions (Mean: 0 = Negative, 1 = Positive)

	Platform compatibility	Optimized for the handicapped	Loading time	Proper display under different resolutions	Support for "third party" components	Tracking mechanism with consent	Privacy statement	Masked email addresses	N
GCC	0.06	0.0	0.0	0.98	0.0	0.5	0.6	0.56	**129**
Bahrain	0.14	0.03	0.0	1.0	0.0	0.0	0.29	0.29	**7**
Saudi Arabia	0.03	0.0	0.0	0.99	0.0	0.56	0.59	0.67	**78**
Kuwait	0.08	0.0	0.0	1.0	0.0	0.83	0.58	0.67	**12**
Qatar	0.0	0.0	0.0	1.0	0.0	0.5	1.0	0.5	**4**
U.A.E.	0.14	0.0	0.0	0.93	0.0	0.32	0.68	0.29	**28**

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Concerning DoS, 21% of the websites show some signs of vulnerability although such an assessment is very difficult to verify. This implies the very low level of quality of some websites and the indifferent attitude of their webmasters. A DoS attack can bring a website completely offline sometimes for days or weeks thus eliminating the credibility of the particular product or company behind it.

The aggregate mean in the case of the websites that time-out by default is also negligent, almost 0. Although not exactly a security issues but it is one of those characteristics that distinguish a well maintained website from the others that are not. The mechanism ensures that the critical web pages containing sensitive data will not stay on the screen for long when the user leaves the computer unattended thus protecting the user from intruders since the page is locked and it needs a fresh login.

The above results lead to, at least, a couple of interpretations both of them negative. The first is that, as it looks, there is no particular strategy planned and followed as to security features implemented for the companies' websites in the region but, quite likely, everything happens on an ad hoc basis. If the developer is skilled, knowledgeable and aware of its importance then it is most likely that s/he will address such issues.

The second is that, quite likely, most marketing experts in the region are not experienced enough to understand the importance of correct online marketing strategies and plan with them in mind and even when they are the webmasters are not skilled enough to implement comprehensive and technically sound web solutions that will be able to address the various issues associated with security provisions of a company's online presence.

4.3 Accessibility, availability and privacy

Figure 4 is, indeed, one picture worth a thousand words. Apparently, the designers and/or developers of the websites evaluated are not seriously interested in addressing any issues related to accessibility and/or availability. Almost none of the websites are loading fast enough, especially on tables/smartphones, as it takes in several cases even more than 20'' to load which is, of course, absolutely unacceptable given the modern technologies. This is mainly because of the non-optimized size of graphics and the lack of modern web design (dynamic web pages etc.). It looks that the designs are focusing more in developing, again, "any" website even barely functional than in producing an effective online solution. Furthermore, but not surprisingly given the low level of overall quality of the products, almost none of them are optimized for handicapped people. Furthermore, 6% of the websites have issues when it comes to different platform compatibility, i.e. different browser and/or OS or device. This suggests those websites are not accessible from all the potential users.

In 56% of the websites the email addresses are unmasked. Nowadays, all email addresses should be protected by scripts or depicted in a graphic element and not as text. Those unmasked addresses can be easily collected by crawlers and used either for spam email or even for phishing attacks.

Half of the websites are using tracking mechanisms without the consent of the user. This means that the websites are utilizing the user's data (private or not) such as IP address, most likely by storing a cookie into the user's computer for reference and personalizing their usage, without the user being aware of this. In many countries of the world today this could be even illegal.

In 40% of the cases there is no privacy statement, which is also a very serious matter. This leaves a lot of room for suspicions that the company might use the data collected from the user (personal or not) for purposes the user is not informed of. This data could be sold or given to third parties for further processing, for advertising purposes, for statistical reasons or even direct market targeting and other activities. In any of the above circumstances, the user should be absolutely aware of how and where the data will be used. Once again it should be noted and cannot be stressed enough that this is a legal obligation in a lot of countries today especially developed ones.

5. CONCLUSION

"…Unfortunately, evaluation of websites is too often neglected by many organizations, public or commercial, and many developers test systems only after they fail or after serious complications have occurred …" [37]. In the case of this research effort the former is probably true instead of the latter if testing is

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

considered at all. The results of the evaluation of the 128 conveniently selected GCC companies' websites are not very encouraging, to say the least. The matter of security does not look to be a very hot topic in the region. A lot of the websites lack basic security attributes leaving security holes wide open and, quite likely, rapidly and dramatically reducing, or even eliminating, the level of trust of their web users.

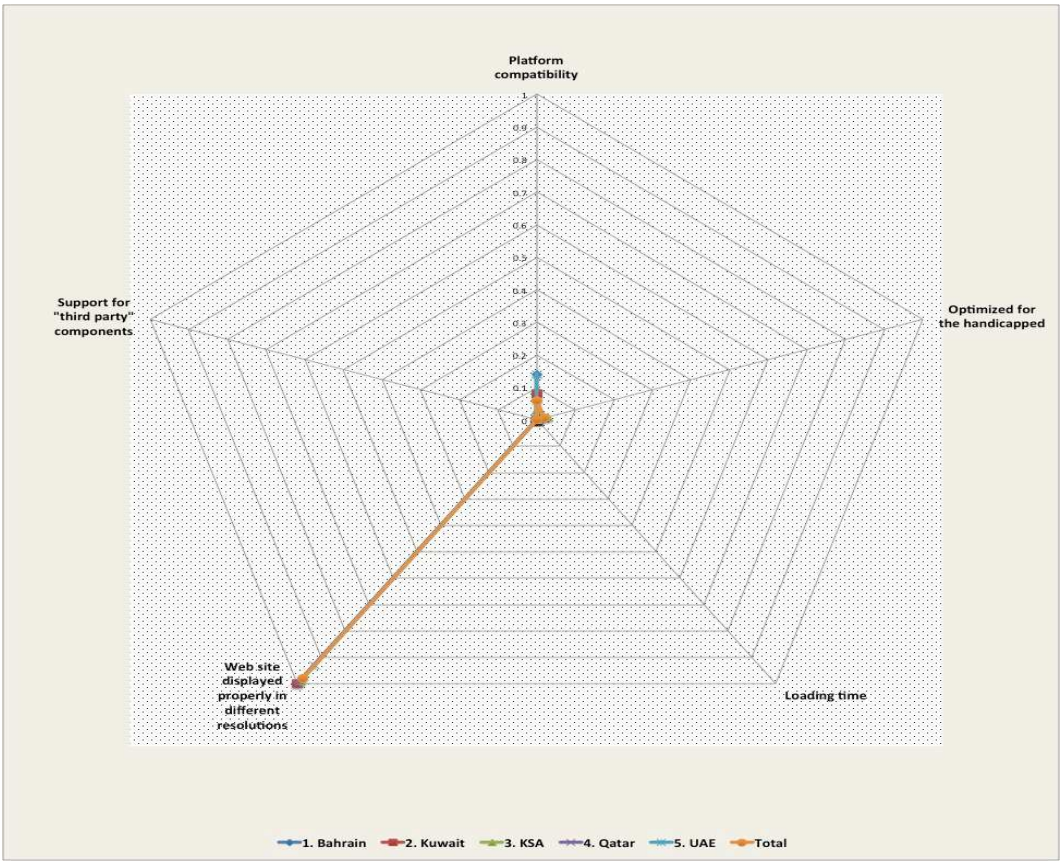

Figure 4. Accessibility And Availability Features

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

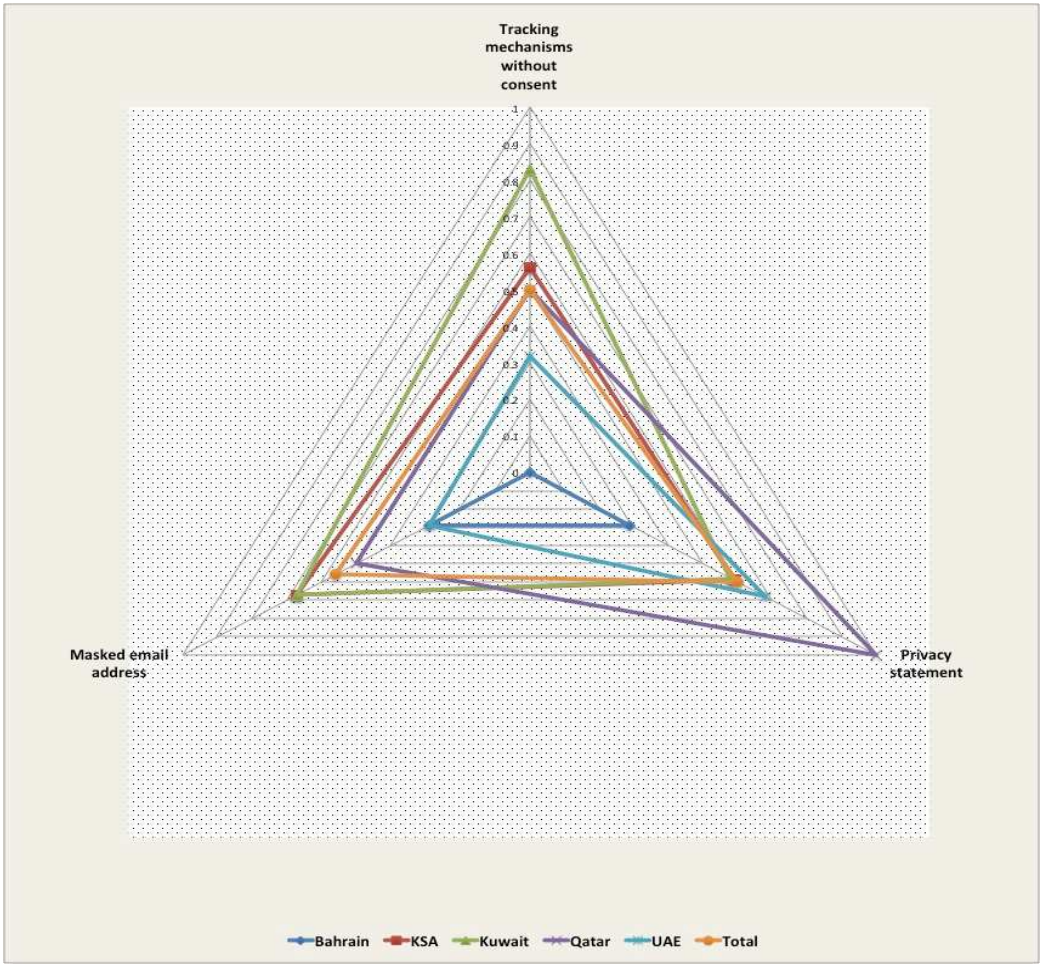

Figure 5. Privacy Features Implemented

There are a lot of websites that look "orphan" or "abandoned", i.e. it is obvious that they are left over without any maintenance resulting in security flaws, misplaced or displaced graphics and text, errors in presenting the data, etc. Those websites are destructive rather than beneficial for the companies they represent.

In general, based on the quality of the websites one can come up with the, rather safe, conclusion that the maturity and effectiveness of the web design strategies of their respected company executives is highly questionable. Companies and any business, government or other entities in general should better realize that a website is neither a luxury nor something that once created there is no need to be dealt with again. It needs constant care, continuous update with new and fresh material, change of topics and themes reflecting the current trends and, most important, keep it up-to-date in addressing new security threads.

ACKNOWLEDGEMENTS

George Violettas wishes to thank TTC for financially and morally supporting this work.

REFERENCES

[1] Go-Gulf. "Internet Usage in the Middle East – Statistics and Trends [Infographic]" [Online], 2014.

[2] Xanthidis, D., Alali, S. A. "Investigating the attitude of the average Saudi towards the Social Media", Proceedings of ACACOS '14, WSEAS, Kuala Lumpur, 2014, pp. 86-94.

[3] Xanthidis, D., Nicholas, D., Argyrides, P. "A Proposed Template for the Evaluation of Web Design Strategies", in *Emerging*

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Markets and e-Commerce in Developing Economies, 2009, pp. 119-144.

[4] Stamm B. S., Markham G, "Reining in the web with content security policy", Proceedings of the 19th International Conference on World Wide Web, ACM, 2010, pp. 921-929.

[5] Giffin D. *et al.*, "Hails: Protecting Data Privacy in Untrusted Web Applications", in 10th USENIX Symposium on Operating Systems Design and Implementation (OSDI), pp. 47-60, 2012.

[6] Kainda R., Flechais I., Roscoe A., "Security and Usability: Analysis and Evaluation", in IEEE, ARES'10 International Conference on., 2010.

[7] Treiblmaier H., Pinterits A., "Developing metrics for Web Sites", *Journal of Computer Information Systems,* 50, 2010.

[8] Vila N., Kuster I., "Consumer Feelings and Behaviors Towards Well Designed Websites", *Information & Management,* Vol. 48, Issue 4-5, May 2011, pp. 166-177, DOI: 10.1016/ j.im.2011.04.003.

[9] Tarafdar M., Zhang J., "Determinants of Reach and Loyalty – A Study of Website Performance and Implications for Website Design", *Journal of Computer Information Systems,* 48 (2), pp. 16-24, 2008.

[10] Flechais I., "Designing Secure and Usable Systems", [PhD Dissertation] University College London, 2005.

[11] Li X., Xue Y., "A Survey on Server-Side Approaches to Securing Web Applications", *ACM Computing Surveys,* Vol. 46, Issue 4, April 2014, in Computer Survey, CSUR 46-54, 2014, DOI: 10.1145/2541315.

[12] OWASP, "XSS (Cross Site Scripting) Prevention Cheat Sheet", [Online]. Available at: https://www.owasp.org/ index.php/ XSS_(Cross-Site-Scripting)_ Prevention_ Cheat_ Sheet.

[13] "Website Security Statistics Report", [Online]. WhiteHat Security, Available at: www.whitehatsec.com/ resource/ stats.html, 2013.

[14] Saxena P., Molnar D., Livshits B., "SCRIPTGARD: Automatic Context-Sensitive Sanitization for Large-Scale Legacy Web Applications", in Proceedings of the 18th ACM Conference on Computer and Communications Security, 2011.

[15] Scholte T. *et al.*, "An Empirical Analysis of Input Validation Mechanism in Web Applications and Languages", in Proceedings of the 27th Annual ACM Symposium on Applied Computing, pp. 1419-1426, 2012, DOI: 10.1145/ 2245276. 2232004.

[16] Weinberger J. *et al.*, "A Systematic Analysis of XSS Sanitization in Web Application Frameworks", in Proceedings of the 16th European Conference on Research in Computer Security, ESORICS'11, pp. 150-171, Springer, 2011.

[17] Medeiros I., Neves N., Correia M., "Automatic Detection and Correction of Web Application Vulnerabilities Using Data Mining to Predict False Positives", in Proceedings of the 23rd International Conference on World Wide Web, pp. 63-74, 2014.

[18] Tsai J. *et al.*, "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study", *Information Systems Research,* Vol. 22, Issue 2, 2010, pp. 254-268.

[19] Anton A., Earp J., Young J., "How Internet Users' Privacy Concerns Have Evolved Since 2002", *IEEE Security and Privacy,* Vol. 8, Issue 1, 2010, pp. 21-27, DOI: 10.1109/MSP.2010.38.

[20] Willis C., Zeljkovic M., "A Personalized Approach to Web Privacy: Awareness, Attitudes and Actions", *Information Management & Computer Security,* Vol. 19, Issue 1 pp. 53-73, DOI: 10.1108/0968522111111.

[21] LaRose R., Rifon N., "Your Privacy is Assured-of being Disturbed: Websites with and without Privacy Seals", *New Media & Society,* Vol. 8, No. 6, pp. 1009-1029, December 2006, DOI: 10.1177/1461444806069652.

[22] Jensen C., Potts C., "Privacy Policies as Decision-Making Tools: An Evaluation of Online Privacy Notices", in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 471-478, 2004, DOI: 10.1145/985692.985752.

[23] Taylor D., Davis D., Jillapalli R., "Privacy Concern and Online Personalization: The Moderating Effects of Information Control and Compensation", *Electronic Commerce Research,* Vol. 9, Issue 3, September

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2009, pp. 203-223, Springer, DOI: 10.1007/s10660-009-9036-2.

[24] Goldfard A., Tucker C., "Privacy Regulation and Online Advertising", *Management Science,* Vol. 57, Issue 1, January 2011, pp. 57-71, DOI: 10.1287/mnsc.1100.1246.

[25] Galletta D., Henry R., McCoy S., Polak P., "Web Site Delays: How Tolerant Are Users?", *Journal of the Association of Information Systems,* Vol. 5, No. 1, January 2004, pp. 1-28.

[26] Sheng H., Lockwood N., "The Effect of Feedback on Web Site Delay: A Perceptual and Physiological Study", in SIGHCI 2011 Proceedings, Paper 11, Available at: http://aisel.aisnet.org/sighci2011/11.

[27] Maxwell D., Azzopardi L., "Stuck in Traffic: How Temporal Delays Affect Search Behaviour", in IIiX' 14 Proceedings of the 5th Information Interaction in Context Symbosium, pp. 155-164, ACM, DOI: 10.1145/2637002.2637021.

[28] Xanthidis D., Alali A. S., Koutzampasopoulou O., "'Stickiness', i.e. HCI Guidelines, Largely Ignored when Developing Web Sites in the GCC", in Proceedings of the 4th IEEE International Conference on Information Science and Technology (ICIST 2014), April 2014, Shenzhen, pp. 801-804, DOI: 10.1109/ICIST.2014.6920598.