The Future of Enterprise Security with Regards to Mobile Technology and Applications

F. T. Tagoe[1] and M. S. Sharif[2,3]

[1]Department of Digital Innovation and Creative Enterprise
GSM London, London, UK
[2]School of Architecture, Computing and Engineering
University of East London, University Way, London, UK
[3]Department of Electronic and Computer Engineering
Brunel University London, Uxbridge, UK
{info@tonishatagoe.com}

Abstract

The utilisation of work assigned mobile technology by enterprise staff to chat and upload contents to the social media applications for personal use has become a key issue for a significant number of enterprises. This work aims to understand the trends amongst the users of work assigned phones when unknowingly downloading and using applications which could breach the security of the enterprise. In this paper; we assess current trends amongst employees and organisations' use and trust of hybrid and web based social media applications used on a daily basis to communicate. This information is then evaluated alongside human related cyber security risks presented by such applications to provide instructions and advice on the management of social media application use within organisations in the Healthcare, Education and Energy sectors. The findings may be employed to develop a more robust cyber security strategy which focuses at reducing the user related risks.

Keywords: Social Media, Security, Mobile Technology.

1. Introduction

According to Accenture, from 2012 to 2013 [1] — the number of social network users around the world rose from 1.47 billion to 1.73 billion (about 25 percent of the world's population), an 18 per-cent increase and this is predicted to rise to 2.55billion in 2017. Aside from this, 77% of Fortune500 companies now have active Twitter® accounts, 70% have Facebook® pages and 69 percent have YouTube™ accounts. "Social networking, user-generated content and PHP-based applications are prevalent on the

web… consider how easily sensitive personal information can be accessed through these channels," said Amichai Shulman, chief technology officer at Imperva [2].

54% of companies had a 100% block on social network use in 2009 but by 2011, this number was reduced to just 31% [3]. With such a fast growing presence online of both individuals and organisations, the benefits of being online and having staff who understand how to use social media effectively is clearly beneficial. The difficulty for cyber security and information security departments is in designing and building effective management systems that can identify legal and strategic risks. Each company will need to make appropriate considerations regarding their consistent voice to suit their objectives and values [4].

1.1 The Internet - Human Right or Utility?

The United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression ruled that removing access to the internet is a human rights violation of article 19, paragraph 3, of the International Covenant on Civil and Political Rights [5]. Aside from providing individuals with the security of knowing their rights are protected, this also went a long way towards encouraging people globally to see the internet as a space to speak freely and share their thoughts [6]. For companies, this has increased the ability of customers to provide feedback and praise on dedicated digital platforms as well as social media sites.

More recently, in early June 2016, the Federal Communications Commission (FCC) in the United States voted on the topic and ruled that High speed Internet is a Utility thereby classifying that phones and power and should be available to all Americans [7]. This perspective aligns with President Obama's Net Neutrality agenda. The majority opinion globally is that there is a need to prevent local governments from deciding which companies can compete to provide internet access by deregulating the industry to encourage competition and innovation [8]. Competition is not always healthy, and some companies around the world have been known to attempt to bribe employees of competitors to share private company information. Organisations need to ensure their staff can be contacted when on the move and that they are able to communicate with each other in order to carry out their jobs [9]. This requires the use of technology and mobile technology plays a large part in this [10].

2 Enterprise & Mobile Technology

2.1 Native Social Media mobile applications

Native applications are developed to work on specific devices and operating systems and as a result are installed directly to the device. Such applications are readily available on all well-known app stores such as the Apple App Store and Google Play and are required to conform to the security requirements of the Marketplace or App Store they will be downloaded from in order to gain approval [11].

As a result, such applications are unable to function across operating systems and must be developed individually to fulfill security requirements of the App store and the Operating System meaning a larger amount of time and money is involved in the development of such tools. This however does provide increased reliability for developers as the SDK and development tools increase the ease of creation.

The benefit of such applications is that they can be used both offline and online and provide a smoother experience through increased speed of use and ubiquitous access [12]. This is possible through a combination of local storage of information and sychronisation when connected to the cloud. Users are also more attracted to such applications as they provide familiar device-specific functionality such as the cameras and accelerometer increasing User Experience fulfilling user expectations.

The disadvantages of such applications are in the time and resources required to develop multiple applications which are able to function on the wide range of devices available on the market today. Alongside this are the in-creased customer support, maintenance costs and extensive approval processes across the various app stores .[13] Many users are unwilling to download such applications onto their devices as company regulations may discourage such activity. These disadvantages present as barriers for developers who strive for popularity amongst users in order to gain a positive return on investment.

2.2 Web Applications

Web applications unlike Native applications are cloud hosted internet-enabled applications such as which can be accessed through web browsers or web service based native clients installed on the device via the app store [14]. Such apps are written with widely recognized programming language such as HTML, CSS, PHP and JavaScript, providing access to a wider set of devices (Windows, iPhone, Android etc) and operating systems with the only requirement being access to the internet reducing the development, maintenance and customer support costs to the developer. Such applications also provide ease of access for users through search engines such as Yahoo and Google as well as website integration through device detection processes.

The benefit of the Web application is the removal of the requirement to submit the application for safety and security approval through App Stores and Marketplaces [15]. This means that the applications can be released at will by developers based on their preferences without consideration for security restrictions imposed by any individual Company and users do not need to go to such Marketplaces to access applications developed in this way.

The disadvantages of mobile web applications however lie mainly in the limited access to device features for functionality of elements such as hand gestures and recognition of sensors and cameras [16]. Furthermore, although there is a reduced requirement to develop different versions of the application for marketplaces, there is a need to consider the various web browsers, versions and the relationships that they have with individual devices thereby making it difficult to develop stable applications which function across devices with minimal issues. With the applications not been advertised in marketplaces and app stores, users are less likely to discover whether applications and when they do quality control, safety and more importantly security are not guaranteed.

Although Web Based applications appear to be safer to use, many include the common PHP script (present in over 75% of websites) which can allow extremely sensitive data to be sourced directly from the phone through file inclusion attacks, once the user uploads content, grants permissions at the point of download or is led to believe they are in the application when they may in fact be using a cloned User interface.

2.3 What are the main sources of risk to enterprise?

Social media is so widely used in modern day, most people fail to take it seriously and as a result regularly download and install social media applications without looking beyond the default settings [17]. This brings rise to risk as lack of this the configuration of setting provide easy access to those conducting social engineering attack identity fraud and attempting to steal confidential information. The Figure 1 shows 11 of the top risks as listed by Gartner in relation to social media.

Risk	Description	Security	Type
Malware	Infection of desktops, propagation of malware through staff or corporate profiles on social-media services.	Yes	Technology
Chain of providers	Mashups of applications within a social-media service enable the untraceable movement of data	Yes	Technology
Interface weaknesses	Public applications interfaces are not sufficiently secured, exposing users to cross-site scripting and other exploits	Yes	Technology
Reputation damage	Degradation of personal and corporate reputations through posting inappropriate content	No	Content
Exposure of confidential information	"Loose lips sink ships," breach of IP or other trade secrets, breach of copyright, public posting or downloading of private or sensitive personal information	Yes	Content
Legal exposure	Legal liabilities resulting from posted content and online conversations or failure to meet a regulatory requirement to record and archive particular conversations	Yes	Content
Revenue loss	For organisations in the information business, making content freely available may undercut fee-based information services	Yes	Content
Staff productivity	Workers failing to perform due to the distraction of social-media	No	Behaviour
Hierarchy subversion	Informal social media networks erode authority in formal corporate hierarchy and defined work processes	No	Behaviour
Social engineering	Phishing attacks, misrepresentation of identity and/or authority to obtain information illicitly or to stimulate damaging behaviours by staff	Yes	Behaviour
Identity fraud	Profiles and postings that are erroneously attributed to a staff member or corporate office	Yes	Behaviour

Source: Gartner (January 2010)

Figure 1: The top 11 risks as listed by Gartner in relation to social media.

Understandably, increasing the level of security on social media account restricts the ability of users being able to be easily found by friends and family and easing his applications to connect with [18]. The issue is about making these accounts more secure without losing functionality, ease-of-use and preventing people from accessing content such as images and Profile pages. This applies to all elements of technology from the mobile handset's preconfigured settings to the individual social media accounts, content and level of access provided to each application. The level of security and user implements is usually based on the level of risk they are willing to take any amount at which they willing to expose themselves online and really a result of deep thought about the security required for or by the company issuing the device.

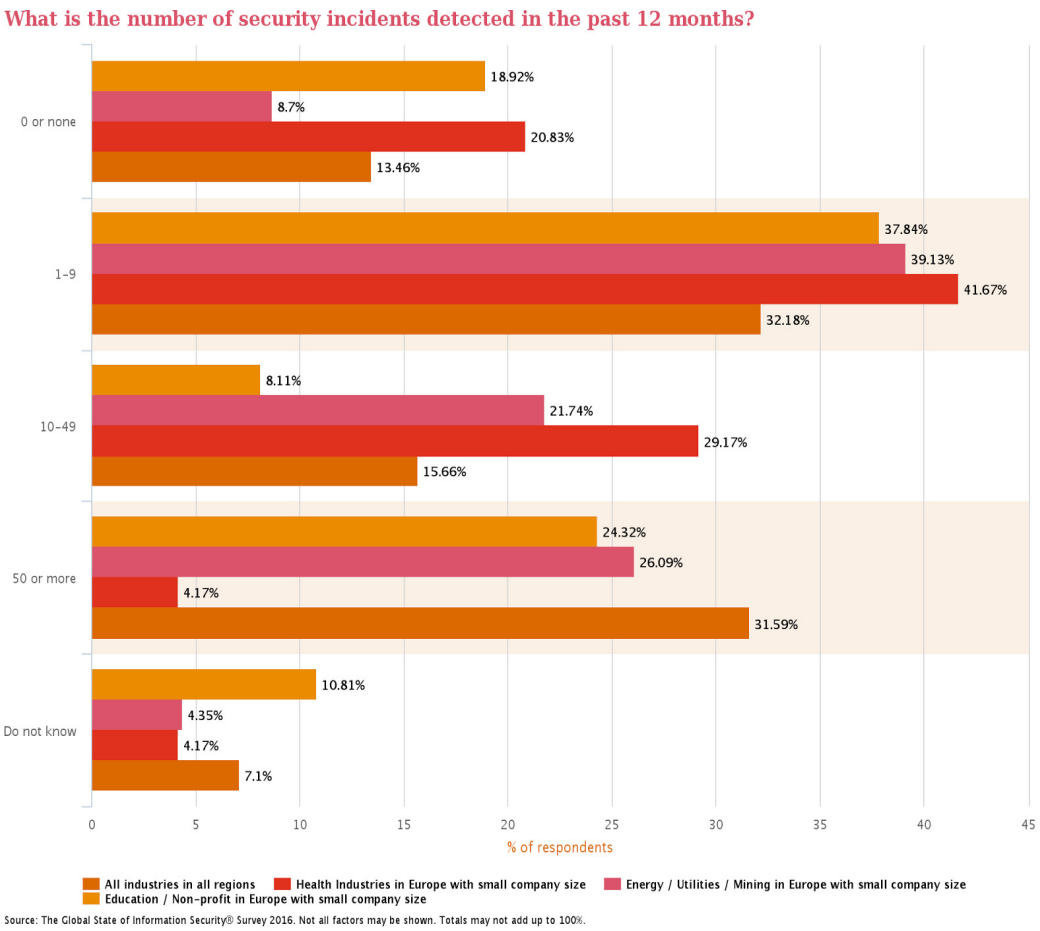

Figure 2: The global State of Information Security Survey 2016, which includes health industres, energy and education.

A recent study into cyber security threats conducted by PWC asked over 100 companies around the world a range of questions about the state of cyber security within their organisations and future plans to increase security.

These results have been filtered for the purpose of sourcing data specific to the three sectors of focus for this paper (Healthcare, Education and Energy) within Europe. In the table above, 31.5% of companies in the education sector reported 50 or more incidents occurring over the previous 12 months. This number is high however, 26.9% of the energy sector participants reported a similar amount.

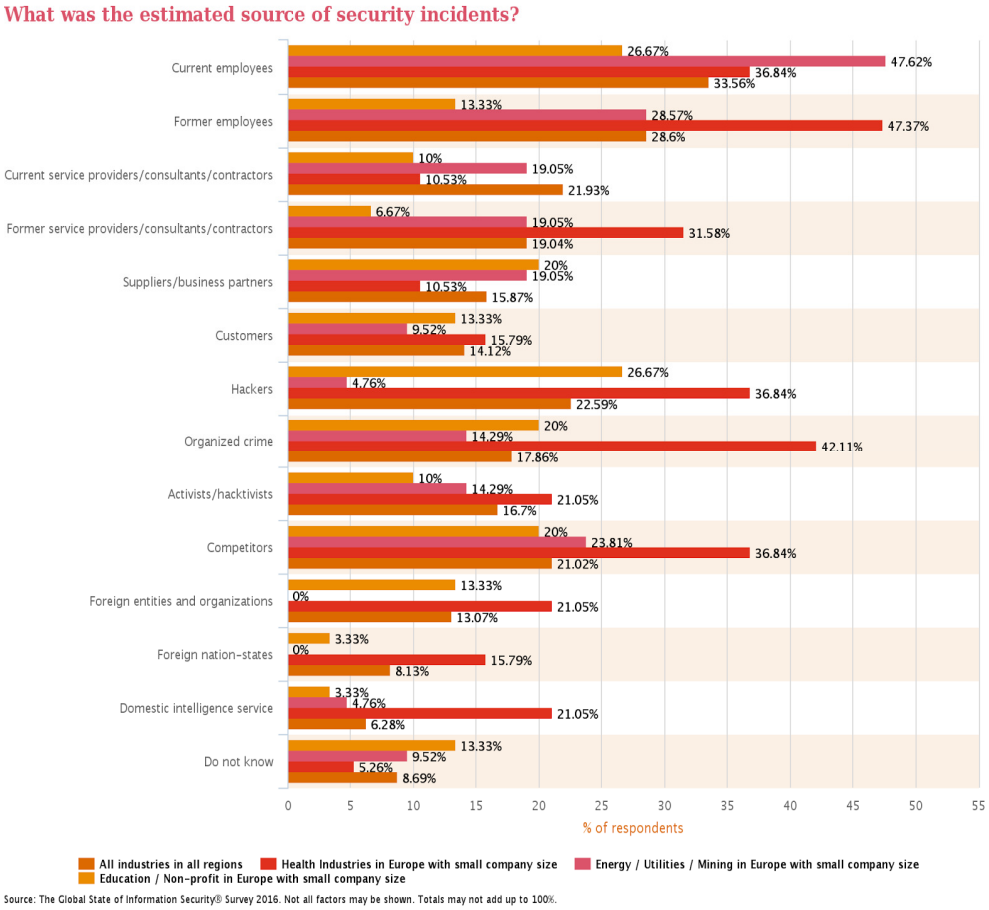

Figure 3: The global State of Information Security Survey 2016, including health industres, energy and education.

Figure 3 shows that current and former employees present the greatest source of incidents with 36.8% of the Healthcare respondents reported employees and while 47.62% of the Energy sector companies reported the highest amount of all threats coming from current employees. Also among the highest responses were from the Energy sector respondents with 42.1% naming organised crime as key sources of incidents over the past year. In contrast to this is the low report of incidents caused by hackers with only 4.7% of the energy sector companies reporting incidents resulting from Hackers.

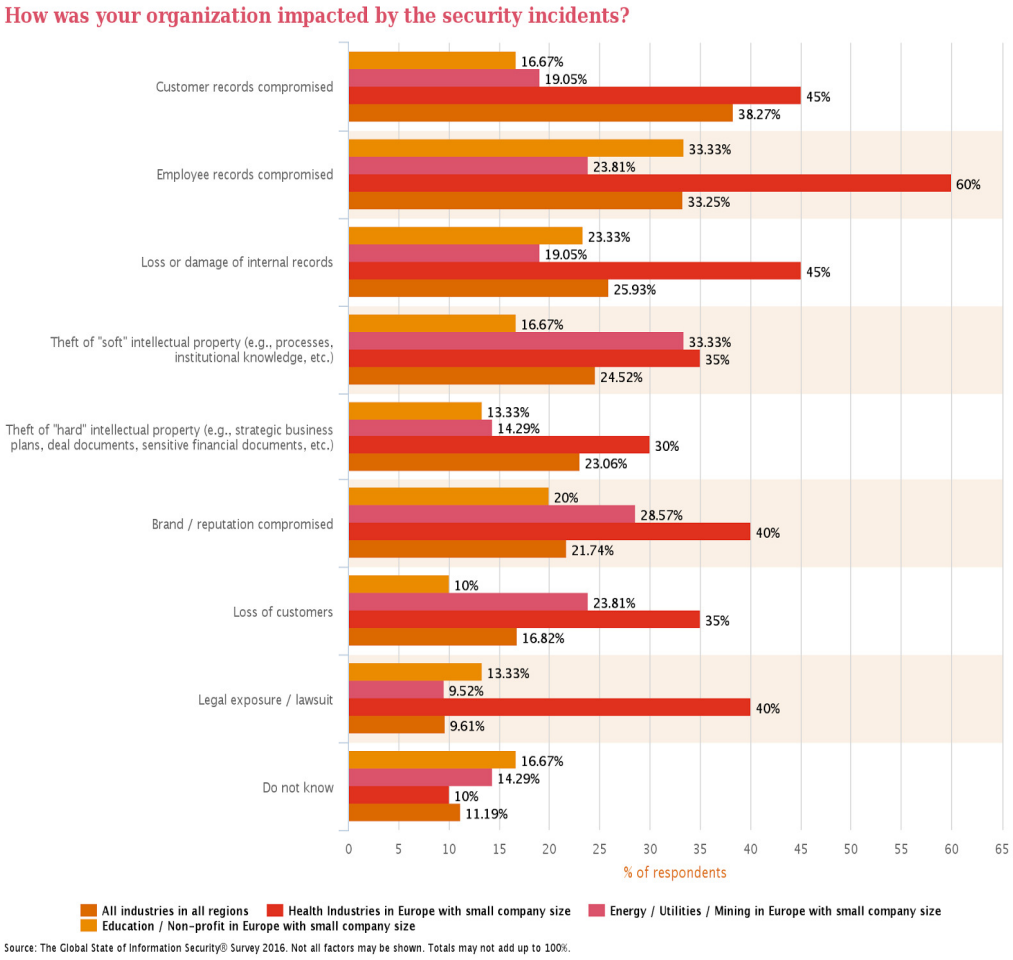

Figure 4: The global State of Information Security Survey 2016, including health industres, energy and education

The impact of the incidents stressed in Figure 4 resulted in consumer, internal and employee records being compromised, theft of intellectual property, reputational damage, loss of consumers and legal exposure. 60% of Energy sector companies reported that employee records were compromised by the incidents.

2.4 The Methodology

The Global State of Information Security Survey in 2016 is a worldwide study by PWC, CIO, and CSO. It was conducted online from the 7th of May 2015 to 12th of June 2015. Readers of CIO and CSO and clients of PWC from around the globe were invited via email to take the survey. The results discussed in this report are based on responses of more than 10,000 CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security practices from 127 countries. Thirty-seven percent (37%) of respondents are from North America, 30% from Europe, 16% from Asia Pacific, 14% from South America, and 3% from the Middle East and Africa. The margin of error is less than 1%.

3 Recommendations for governance and use of Social Media within Enterprise

3.1 Understand the risks through regular bespoke risk assessments

The environment is constantly changing and Hackers are in a position to know more about the device than the manufacturers, distributing companies and staff. Companies have reduced the security restrictions on mobile devices and in some cases remove them in favour of increasing the user experience for staff members.

Two steps verification combined with Single-Sign-On means that once a user is logged into a device which is then stolen or goes missing, not only is there an issue that the data on the device can be accessed; it is possible that someone could access other areas of the company system/database/information using the single sign on feature. Risk assessments and audits should be bespoke to the needs of the specific company and staff requirements.

3.2 Effective management of identified risks

Google play recently changed the rules on how permissions are granted when downloading applications by removing the requirement to grant permissions before users have begun utilising the applications and Whatsapp have recently launched end-to-end encryption protecting user messages from being decrypted.

3.3 Follow and share examples of best practice

Learning from previous cyber security incidents can play a large role in enabling security managers to gain a foothold on the best strategy to implement as the company however considering that on a daily basis over 5 Petabytes of information such as People's attitudes location images and intentions uploaded to the Internet, it is clear the employees amongst others are regularly leaving traces of information on social media platforms. This same information is regularly used by companies to source insights on client and target audiences however this social intelligence is also available to those who wish to use it to target IT and data infrastructure of the organisation. There is also

made a great foundation within the area of risk management, and therefore learning from best practice and developing new methods upon this layout information is fundamental.

3.4 Ensure engagement from the organisation's leadership team

Many cases of Governments and law enforcement operatives obtaining encryption keys from companies and website owners and so ensuring that the leadership team across all levels of the organisation are actively engaged in the process of regularly assessing the situation. Social media is clearly a requirement in the business world today as the marketing methods and dynamics have grown to involve and require the use of social media marketing tools and applications on a day-to-day basis for both private and corporate use. As a result, the changing landscape of business is further complicated by the addition of social media. It is vital that companies adhere to or develop policies around the encryption and decryption of content on work assigned devices.

3.5 Train the Employees, including those without work assigned technology

Staff who are provided mobile devices are in the most part extremely responsible. It is vital that staff is trained and able to understand security threats and best practise regarding the form of information which can/should be stored on mobile devices. Users frequently visit websites via links which could pose a security risk and as a result put employer's data at risk. Poor password selection can be combatted through the use of 2-step verification in conjunction with single sign on services (SSO) such as Security as Service (SAAS) combinations. However, an employee misplacing an unlocked mobile device and another that conducts a malicious information leak presents the same amount of risk. Disgruntled employees with an in-depth knowledge of technology and mobile security can be a serious source of risk.

4 Conclusion and Future Work

The current trends amongst employees and organisations' use and trust of hybrid and web based social media applications used on a daily basis to communicate have been assessed. This information is then evaluated alongside human related cyber security risks presented by such applications to provide instructions and advice on the management of social media application use within organisations in the healthcare, education and energy sectors. The findings can be employed to develop a more robust cyber security strategy which focuses at reducing the user related risks. The vast amounts of information and possible discussions about the risks to enterprise from social media are not fully discussed. However, this relies heavily on the fact that the full of the risks faced by businesses and the possible impacts are not yet being shared enough across business. The data and findings from the PWC survey clearly shows that a large percent of companies (more than 10%) has said that they either do not know if they have had any cyber incidents in the previous 12 months or that they are not aware of the impacts and/or financial losses incurred as a result.

It is vital that the future of business includes the commitment of all employees to maintaining and preserving security both of themselves as individuals and as of the organisation itself. The education, energy and health sectors have a lot to lose through cybercrime that fracture employee and customer data. As a result, managers and leaders must be forward thinking and work towards developing strategies and infrastructure that prevents and mitigates the most common risks at a minimum level.

The while it is clear that social media as with all elements of the Internet are advancing at a faster pace than most are able to grasp from a security perspective, the rewards of engaging these platforms in ways that allow businesses to engage their audience is safely while will provide untold benefits to all involved. A fundamental factor required for this to take place, is honesty and transparency across industry sectors about incidents which have occurred so that (E lessons can be learned and up-to-date training and information can be distributed as often as necessary.

The work presented in this paper establishes the basis for further research activities and findings in the near future. Our future work will involve gathering effective statistics about the most ten popular apps being downloaded by staff onto mobiles (e.g tinder) via the technical department of 100 companies. Then we are planning to analyse the ranking of all apps into order from most to least secure apps. Afterwards these apps will be rated accordingly based on different factors such as threats raised, hack attempts etc. Moreover, a technical based solutions and recommendations will be developed to help and support enterprise. This will lead to develop a global system that provides updated training materials and alerts about the recent breaches to all work based phones. This system will be able to provide advice on the need for increased training and governance for all the employees involved in such work.

References

[1] "Accenture Comprehensive Approach Managing Social Media Risk Compliance.

[2] "Research shows dangers of user-generated content," *ComputerWeekly*. [Online]. Available: http://www.computerweekly.com/news/2240150785/Research-shows-dangers-of-user-generated-content. [Accessed: 28-Jul-2016].

[3] R. Shullic, "Risk Assessment of Social Media," *The SANS Institute*, 2012.

[4] D. Jayaram, A. K. Manrai, and L. A. Manrai, "Effective use of marketing technology in Eastern Europe: Web analytics, social media, customer analytics, digital campaigns and mobile applications.," *Uso Eficaz Tecnol. Mark. En Eur. Este Analíticas Web Medios Soc. Analítica Clientes Campañas Digit. Apl. Móviles*, vol. 20, no. 39, pp. 118–132, Dec. 2015.

[5] "U.N. Report Declares Internet Access a Human Right | WIRED." [Online]. Available: https://www.wired.com/2011/06/internet-a-human-right/. [Accessed: 28-Jul-2016].

[6] S. PREIBUSCH, "Privacy Behaviors After Snowden.," *Commun. ACM*, vol. 58, no. 5, p. 48, May 2015.

[7] C. Kang, "Court Backs Rules Treating Internet as Utility, Not Luxury," *The New York Times*, 14-Jun-2016.

[8] "No, the Internet Is Not a Utility," *Conservative Review*. [Online]. Available: https://www.conservativereview.com/commentary/2016/06/no-the-internet-is-not-a-utility. [Accessed: 28-Jul-2016].

[9] K. Jenab and S. Moslehpour, "Cyber Security Management: A Review.," *Bus. Manag. Dyn.*, vol. 5, no. 11, pp. 16–39, May 2016.

[10] L. Gardner, "Welcome to the Web World.," *J. Aust. N. Z. Inst. Insur. Finance*, vol. 38, no. 3, pp. 1–6, Sep. 2015.

[11] A. CHARLAND and B. LEROUX, "Mobile Application Development: Web vs. Native.," *Commun. ACM*, vol. 54, no. 5, pp. 49–53, May 2011.

[12] R. S. Dikhit, "Using Android for the Enterprise.," *Open Source You*, vol. 4, no. 5, p. 49, Feb. 2016.

[13] "HTML5 vs Native Whats a Mobile Developer to Do 648997," *eWeek*, 2012.

[14] I. de M. Barroca Filho and G. S. Aquino Júnior, "Development of mobile applications from existing Web-based enterprise systems.," *Int. J. Web Inf. Syst.*, vol. 11, no. 2, p. 162, Apr. 2015.

[15] "The Enterprise Guide to Developing Secure Mobile Apps.," *Comput. Wkly.*, pp. 1–19, Jun. 2016.

[16] D. BREWER, "Native apps vs. Web apps.," *N. H. Bus. Rev.*, vol. 33, no. 22, p. 30, Oct. 2011.

[17] A. Gatlin, "Social Media Privacy Settings Get Few Likes From Millennials Show High Level Of Distrust But survey finds gen Yers still need to improve their cybersecurity awareness," *Investor's Business Daily*, 2015.

[18] "Cyber security: Strategies: Comment: Social media is revolutionary, but it can damage your business," *The Guardian (London, England)*, 2013.