JOURNAL OF EDUCATION FOR BUSINESS, 90: 458–466, 2015

ISSN: 0883-2323 print / 1940-3356 online
DOI: 10.1080/08832323.2015.1095705

Routledge
Taylor & Francis Group

Security and Vulnerability Assessment of Social Media Sites: An Exploratory Study

Jensen Zhao
Ball State University, Muncie, Indiana, USA

Sherry Y. Zhao
Massachusetts Institute of Technology, Cambridge, Massachusetts, USA

While the growing popularity of social media has brought many benefits to society, it has also resulted in privacy and security threats. The authors assessed the security and vulnerability of 50 social media sites. The findings indicate that most sites (a) posted privacy and security policies but only a minority stated clearly their execution of the key security measures; (b) had network information that was publicly available through Internet search, which was vulnerable to cyber intrusion; and (c) were secured with firewalls, filters, or port closures, with only few ports detected as open, which need further improvement.

Keywords: computer network systems, social media, security, vulnerability

The world has witnessed how the Internet-based social media, such as Facebook, Twitter, and YouTube, have changed the traditional communication landscape and empowered people to play active roles in economic, social, and political activities. Empowered with social media, consumers are increasingly active in cocreating everything from product design to promotional messages; they want companies to listen, appropriately engage, and respond (Berthon, Pitt, McCarthy, & Kates, 2007; Kietzmann, Hermkens, McCarthy, & Silvestre, 2011). For instance, acting on behalf of her 4-year-old brother who loves to cook and wanted an oven, McKenna Pope, a 13-year-old girl got more than 40,000 signatures on her online petition at Change.org requesting the toy maker of the Easy-Bake Oven to make a version for both boys and girls. In response, the manufacturer of the Easy-Bake Oven (Hasbro, Pawtucket, RI), a toy marketed only to girls over its 50-year history, accepted the petition to make a gender-neutral oven and to include boys in the ads starting in 2013 (Cavaliere, 2012).

The top U.S. marketers at *Fortune* 100 and *Forbes* Top 200 companies indicated that the social media spending was 3.5% of company marketing budget on average in 2009 and increased to 7.4% of the marketing budget in 2012. The top U.S. marketers expected that the social media spending would reach 19.5% of their marketing budgets in five years following 2012 (Moorman, 2012). Research also indicated that the proper corporate use of social media impacts positively the corporate revenue and profit (Zhao & Zhao, 2014).

However, the growing popularity of social media on the Internet has also resulted in privacy and security threats to people, businesses, and governments. For instance, a Nexgate's cyber-threat analysis of the social media presence of the *Fortune* 100 firms from July 2013 to June 2014 reported that, on average, one in five Twitter accounts and two of five Facebook accounts claiming to represent a *Fortune* 100 brand were unauthorized. On aggregate, *Fortune* 100 brands experienced at least one compromise every day on their social media accounts (Ashford, 2014a). In 2014, 70% of social media scams were manually shared and these scams spread rapidly and were lucrative for cybercriminals because people were more likely to click something posted by a friend (Symantec, 2015).

As research showed, some social media sites were compromised by hackers; celebrities' private pictures, personal information, and emails were published by hackers on the web (e.g., Ashford, 2014b; Gay, 2014; Nerney, 2011). These attacks mainly targeted at networks' TCP/IP (Layer

Correspondence should be addressed to Jensen Zhao, Ball State University, Miller College of Business, ISOM Department, Muncie, IN 47306, USA. E-mail: jzhao@bsu.edu

Color versions of one or more figures in this article are available online at www.tandfonline.com/vjeb.

4), secure socket layer (SSL; Layer 5), and HTTP and FTP (Layer 7) according to the Open Systems Interconnection Reference Model (McNurlin & Sprague, 2006). Overall, cyber attackers' primary purpose of social media intrusion and attack is to steal customer data, defame celebrities, damage brands, and manipulate markets for financial gains (Ashford, 2014a; Symantec, 2015). According to the Trustwave Global Security Report, cybercrime gave attackers 1,425% return on investment (Trustwave, 2015).

The purpose of the present study was to assess the security and vulnerability of the social media sites by examining the following issues: the privacy and security policies and implementations, information availability of social media systems, computer network security of social media sites, and the difference of privacy and security measures between U.S.-based social media sites and other country-based counterpart sites. Four research questions guided this study:

Research Question 1 (*RQ1*): What privacy and security measures are stated in policies on the social media sites?

RQ2: What network information of social media sites is publicly available on the Internet?

RQ3: How secure are the computer network systems of the social media sites to cyber intrusions and attacks?

RQ4: How do the U.S.-based social media sites differ from other country-based counterparts in securing their sites?

The findings of the study would benefit the social media administrators for continuous improvement of their social media security. In addition, the findings would enable students specialized in e-business or Internet security to identify opportunities for internships or jobs at the social media sites that need to strengthen or maintain their Internet security. As the 2014 *Occupational Outlook Handbook* (Bureau of Labor Statistics, 2014) indicated, the employment of information security analysts was projected to grow 37% from 2012 to 2022, much faster than the average for all occupations. Demand for information security analysts is expected to be very high as these analysts will be needed to come up with innovative solutions to prevent hackers from stealing critical information or creating havoc on computer networks.

METHOD

To assess social media sites in terms of (a) privacy and security policies and their implementation, (b) network information availability of social media sites, and (c) computer network system vulnerability to cyber intrusions and attacks, we used three methods for data collection and analysis: web content analytics, network system information auditing, and computer network security mapping.

The web content analytics is commonly used in assessing organizations' web contents, deliveries, and strategies (e.g., Boggs & Walters, 2006; Campbell & Beck, 2004; Wilkinson & Cappel, 2005; Zhao & Zhao, 2004; Zhao, Truell, Alexander, & Davis, 2006). We used this method for systematically and objectively identifying and recording the privacy and security policies available at the social networking sites and then analyzing what privacy and security measures were stated as in implementation. This method generated the following content categories for analysis: (a) existence of privacy, security, child-protection, proper-use, and no-liability policies; (b) antihacking notice; (c) data transmission encryption; (d) intrusion detection; (e) investigation of improper web activities; (f) login authentication; and (g) web traffic monitoring.

To find out what network information of the social media sites is publicly available on the Internet and how vulnerable the social media sites are to cyber intrusions and attacks, we conducted Google search for related websites and auditing tools. We found three websites—ZoneEdit.com, arin.net, and insecure.org—offering the tools.

The ZoneEdit.com site is a leading website in DNS (Domain Name System) and domain management solutions. It provides a free DNS lookup utility tool, which enables any online user to enter a website domain name (e.g., yahoo.com) for searching its IP (Internet Protocol; e.g., 216.115.108.245) address (see at http://www.zoneedit.com/lookup.html).

The arin.net (American Registry of Internet Numbers) site provides a free database search service at ws.arin.net. The search service allows any online user to find a website's registration information for resources registered with ARIN. The ARIN database contains IP addresses, autonomous system numbers, network name, type, and range, organizations or customers that are associated with these resources, and related points of contact. By entering a site's IP address into the search tool, any person can get all the registered information of the site's network systems (see at http://www.arin.net/whois/).

The computer network security mapping is a major method of using software tools for assessing the vulnerability of an entire computer network system without intrusion and identifying areas of potential security threats (e.g., Garcia, 2004; Winkler, 2004). To assess the vulnerability of the computer network systems of social media sites, we selected a popular, free network mapping utility tool, Nmap, provided by the insecure.org. Nmap is a port scanning and network mapping software. It uses raw IP packets to determine what hosts are available on the network; what ports are open, filtered, firewalled, or closed; what services and servers those hosts are offering; what operating systems they are running; and many other characteristics.

To ensure that using Nmap for this study is legal and ethical, we reviewed related literature and could not find federal or state laws that specifically address the issue (e.g., U.S. Department of Justice, 2003). However, in a Georgia District Court case of Moulton v. VC3, the judge declared a port scan in the case legal because it did not impair the integrity nor availability of the network. The judge found that since the activity performed no damage to the target, it could not be illegal (Jamieson, 2002). The implication of this case is that a port scan is not an attack and usually causes no damage to a target network; the legality and ethics of a port scan depend on whether the intent of a port scan is to cause damage or to improve security. As the purpose of this study was to provide the social media sites' administrators with the findings that they need for continuous improvement of their site security, using Nmap for this study was justified.

The population of this study consisted of the 210 active social media sites around the world, which were ranked by Alexa.com—an amazon.com company specialized in web rating and analytics. This exploratory study randomly selected a sample of 50 social media sites from the population. The sample consists of 35 sites (70%) based in the United States of America and 15 sites (30%) based in other countries such as Argentina, China, Germany, Japan, Mexico, Saudi Arabia, or Spain.

All the data were collected electronically between January and April 2015. The results of web content analytics, network information auditing, and computer network security mapping were saved in digital format and coded for statistical analysis with IBM SPSS. Frequency counts, percentage distributions, means, and standard deviations were prepared. The independent *t* test was employed to identify whether any significant difference existed at the .01 alpha level between the U.S.-based social networking sites and other country-based counterparts in securing their sites in order to address Research Question 4.

TABLE 1
Social Media Sites' Security Measures Stated on Their Sites ($N = 50$)

Policy status	Frequency	Percentage
A privacy policy link present on the site	46	92
A child-protection policy link present on the site	45	90
A no-liability note attached to the security policy or disclaimer	45	90
A proper-use note attached to the security policy or disclaimer	41	82
A security policy link present on the site	41	82
Security measures		
Encryption: using secure socket layer (SSL) encryption to protect data transmissions	37	74
Authentication: using username and password to protect for account privacy and security	12	24
Antipassword guessing: limiting login to 3 trials only	4	8
Monitoring: using software programs to monitor traffic	2	4
Investigation: investigating improper activities to identify individual persons	1	2
Auditing: identifying unauthorized attempts to upload or change information	1	2

FINDINGS

The findings of the study are reported in the following sequence: (a) privacy and security policies on social media sites, (b) network information publicly available on Internet, (c) security status of social media systems, and (d) difference between U.S.-based and other country-based social media sites.

Privacy and Security Policies on Social Media Sites

RQ1 asked, "What privacy and security measures are stated in policies on the social media sites?" As Table 1 shows, of the 50 social media sites, 46 sites (92%) provided a link on their home pages to the privacy policy, but the name of the link varied, and included privacy policy, privacy information, policies, and data use policy. Forty-five sites (90%) presented a child-protection policy link on their home pages or embedded it within the privacy policy. Forty-five sites (90%) also presented a no-liability statement as the disclaimer or attached to the security policy. For example, Facebook's no-liability disclaimer (see Figure 1) stated, "We will not be liable to you for any lost profits or other consequential, special, indirect, or incidental damages arising out of or in connection with this statement or Facebook, even if we have been advised of the possibility of such damages."

Among the 50 social media sites, 41 sites (82%) provided a link on their home pages to the security policy as well as a proper-use note that was attached to the security policy or disclaimer. The security policies indicated that the social media sites are committed to ensuring a secure environment that can protect personal and business information by implementing various security measures (see, for example, Figure 2). While the majority sites (74%) stated using SSL encryption to protect data transmissions, only a minority of the sites stated clearly the execution of the following key security measures: authentication, using username and password authentication to protect for account privacy and security (24%); antipassword guessing, limiting login to three trials only (8%); monitoring, using server management software to monitor traffic (4%);

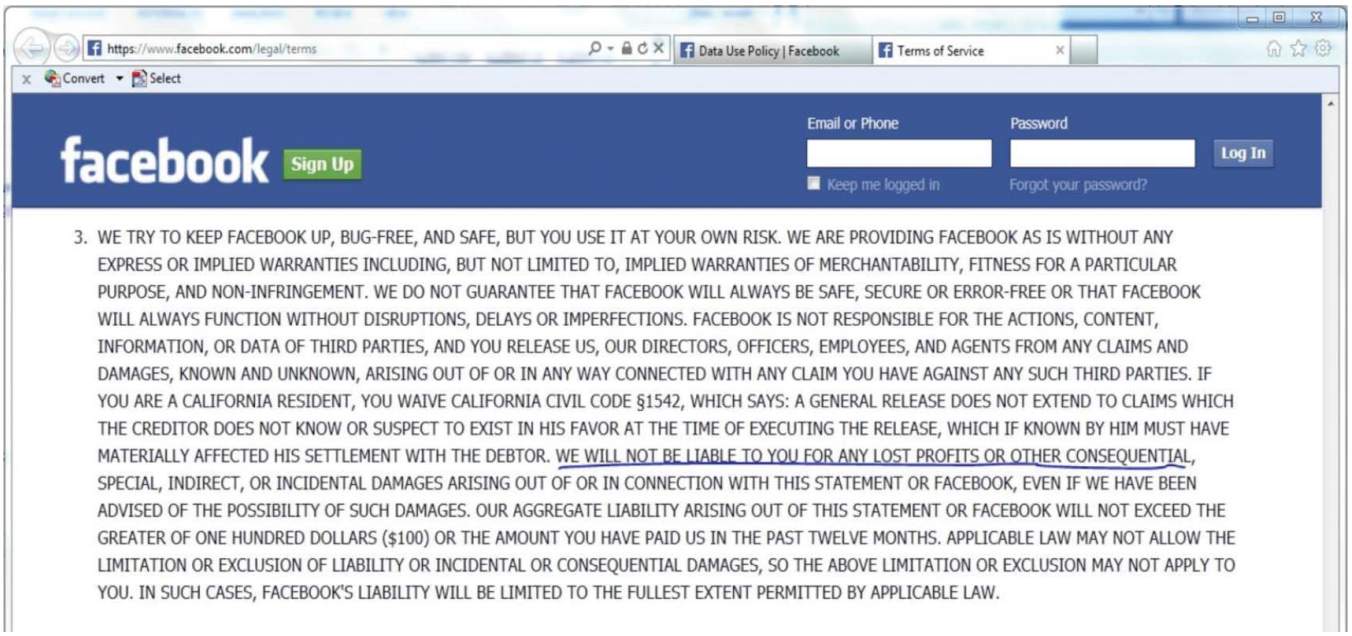

FIGURE 1. No-liability statement at Facebook site.

investigation, investigating improper activities to identify individual persons (2%); and auditing, using intrusion detection software to audit and identify unauthorized attempts to upload or change information or otherwise cause damage (2%).

Network Information Publicly Available on the Internet

RQ2 asked, "What network information of social media sites is publicly available on the Internet?" The Internet search at ZoneEdit.com and ws.arin.net identified the IP

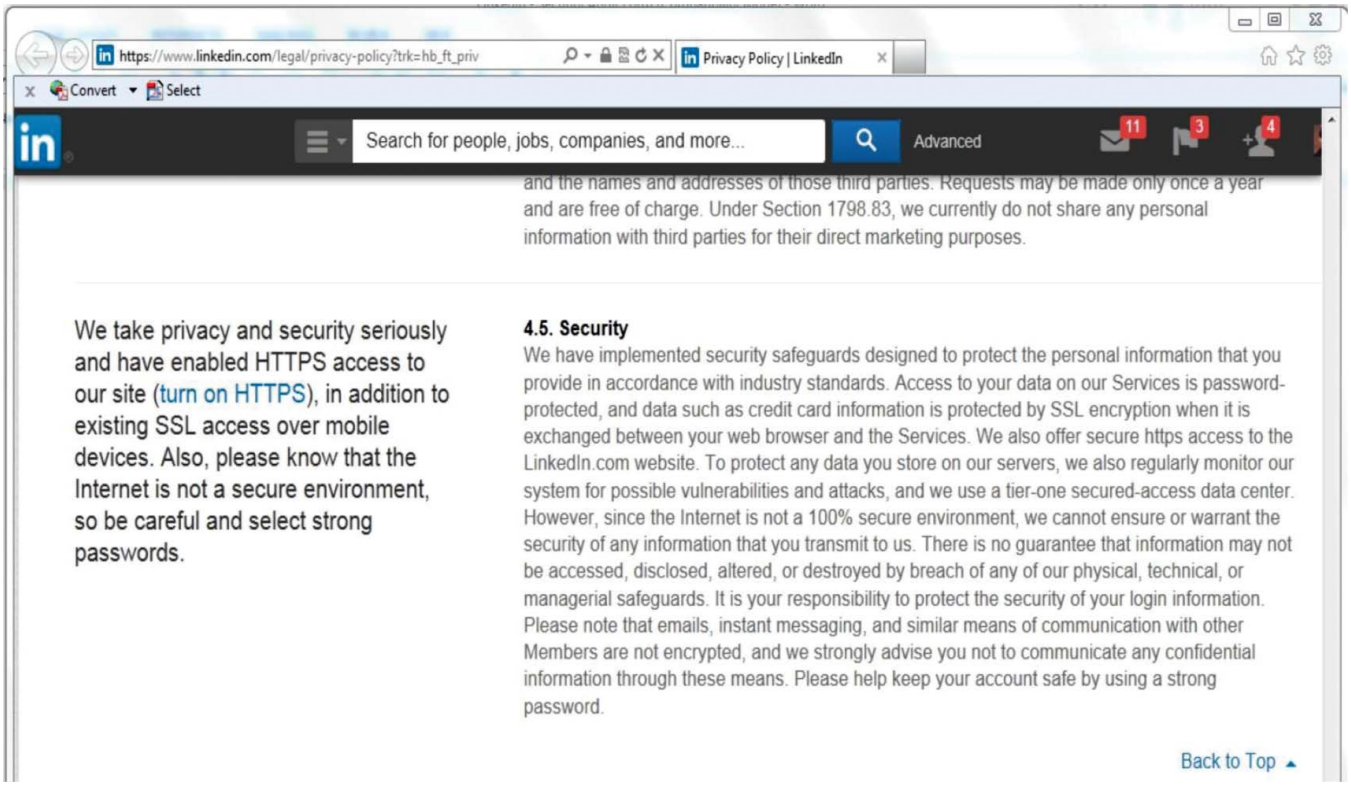

FIGURE 2. Security statement at LinkedIn site.

addresses and network information of almost all the 50 social media sites. As Table 2 shows, 100% of social media sites' IP addresses were publicly available on the Internet. As a consequence, with these publicly available IP addresses, any online users could go to ws.arin.net and enter the IP addresses for identifying a large amount of network information from the majority of the social media sites, such as a site's organization name; physical address; network range, name, handle, type, parent, and CIDR (classless interdomain routing); registration date, last updated time, phone number, email address, and comments (see Table 2).

Security Status of Social Media Network Systems

RQ3 asked, "How secure are the computer network systems of the social media sites to cyber intrusions and attacks?" Computer network systems connect to the Internet through communication ports. The ports of an Internet-connected computer are classified into three categories: (a) the well-known ports, (b) the registered ports, and (c) the dynamic or private ports. The numbers of the well-known ports range from 0 to 1023; those of the registered ports are from 1024 through 49151; and those of the dynamic or private ports range from 49152 to 65535. If the ports are open on the Internet without firewalls or filters, they are very vulnerable to cyber intrusions and attacks. As Table 3 illustrates, of the 50 social media sites scanned by using Nmap, the majority (68%) of the sites revealed only one or two open ports at their respective sites. By contrast, only the minority of the sites revealed three or more open ports. While 13 sites (26%) were detected three or four open ports, only three sites (6%) revealed five, 10, and 26 open ports on their respective sites.

The Nmap scan report also indicated that most social media sites' Internet ports were filtered or behind firewalls. As Figure 3 shows, while Nmap scan did not detect any port information at five social media sites (10%), it reported that four sites (8%) had around 150 ports filtered or behind firewalls and the majority of the sites (82%) had filtered or firewalled their 925 up to 1,000 ports, respectively.

TABLE 2
Social Media Network Information Publicly Available on the Internet

Category	Frequency	Percentage
IP addresses	50	100
Organization name	50	100
Address (city, state/province, country)	50	100
Network range	50	100
Network name	50	100
Network handle	50	100
Network type	50	100
CIDR (Classless Interdomain Routing)	50	100
Registration date	50	100
Last updated	50	100
Phone number	50	100
Email address	50	100
Network parent	39	78
Comments	33	66

TABLE 3
Number of Internet Ports Open at Social Media Sites

		Group	
Open ports	Sites	Frequency	Percentage
1	1		
2	33	34	68
3	7		
4	6	13	26
5	1		
10	1		
26	1	3	6
Total	50	50	100

Regarding the types of open Internet ports, 49 sites (98%) had their Port 80/TCP open for HTTP (hypertext transfer protocol) or world wide web services (see Figure 4). Web servers identified from Port 80/TCP were Apache, Microsoft IIS, and Netscape. Second, 46 sites (92%) also had Port 443/TCP open for encrypted https services. In addition, a minority of the sites had the following ports open for varied purposes: Port 8080/TCP open for http-proxy—a more secure web service than Port 80/tcp (12%), Port 53/TCP open for DNS domain service (6%), Port 22/TCP open for email communication (6%), Port 21/TCP open for FTP file transfer (4%), and Port 8443/tcp open as a https-alternative for encrypted data transmissions (4%).

The Nmap scan also reported the server information and operating systems at the 50 social media sites. As Figure 5 shows, while 20% of the sites did not reveal any match of computer server information, 80% were detected of running varied servers such as Nginx (34%), Apache (24%), AkamaiGHost (6%), ATS (4%), Varnish (4%), Haproxy (2%), GFE (2%), H3rr (2%), and PWS httpd (2%). However, the Nmap scan did not detect computer operating systems at the majority of the sites (70%, see Figure 6). But the minority of the sites (30%) were detected as running Linux (18%), Dell (6%), MS Windows (4%), and NetDBS (2%), respectively.

Difference Between U.S.- and Other Country-Based Social Media Sites

RQ4 asked, "How do the U.S.-based social media sites differ from other country-based counterparts in securing their sites?" As Table 4 shows, in comparison with other country-based social media sites, the U.S.-based counterparts had significantly more secure measures in the following six aspects: (a) child protection policy, $t(48) = 4.099$, $p < .000$; (b) privacy policy, $t(48) = 3.495$, $p < .001$; (c) SSL encryption, $t(48) = 2.961$, $p < .005$; (d) security

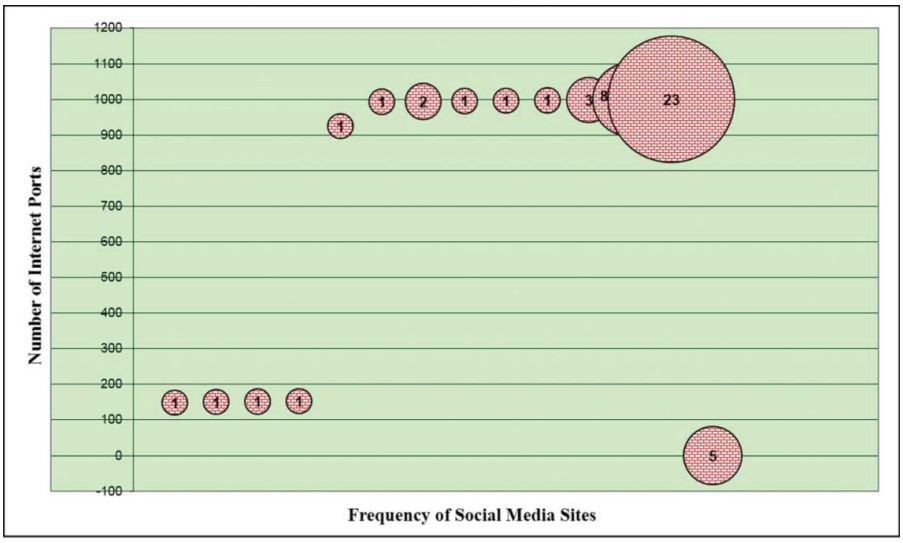

FIGURE 3. Number of internet ports filtered or firewalled at social media sites.

policy, $t(48) = 2.802$, $p < .007$; (e) proper use statement, $t(48) = 2.802$, $p < .007$; and (f) no-liability statement, $t(48) = 2.705$, $p < .009$.

SUMMARY AND CONCLUSIONS

The majority of the social media sites posted links to privacy policy, child-protection policy, no-liability statement, security policy, and proper-use guidelines on their home pages. The majority of the security policies stated using SSL encryption to protect data transmissions. But only a minority of the sites stated clearly the execution of the key security measures: authentication, antipassword guessing, monitoring, investigation, and auditing. These findings indicate the need for further improvement because around 10–18% of the social media sites failed to post the privacy- and security-related policies. In addition, many sites need to clearly state what key security measures are in execution as an effective communication to not only assure users of

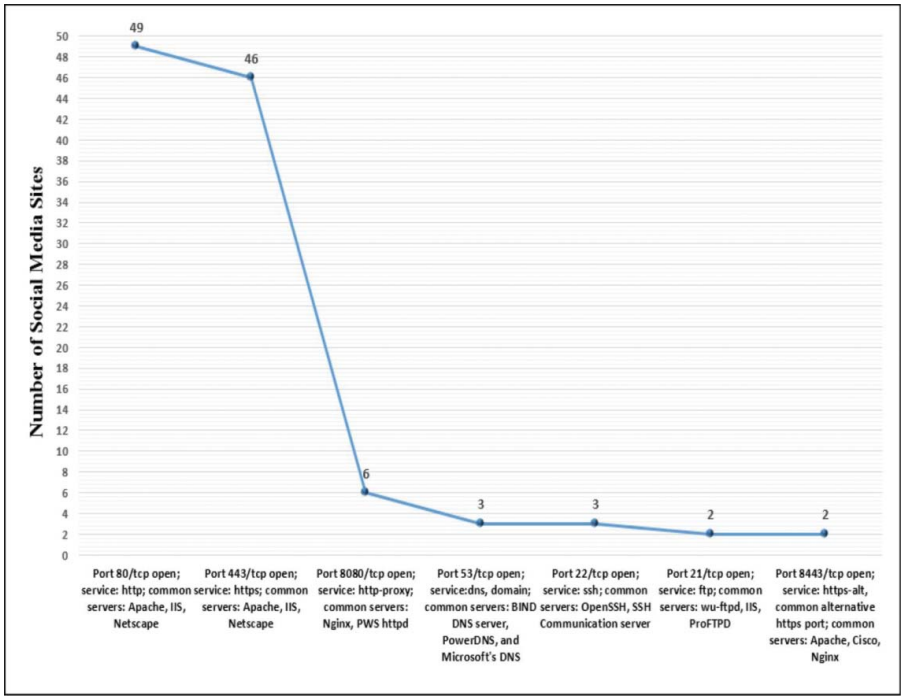

FIGURE 4. Types of internet ports open at social media sites.

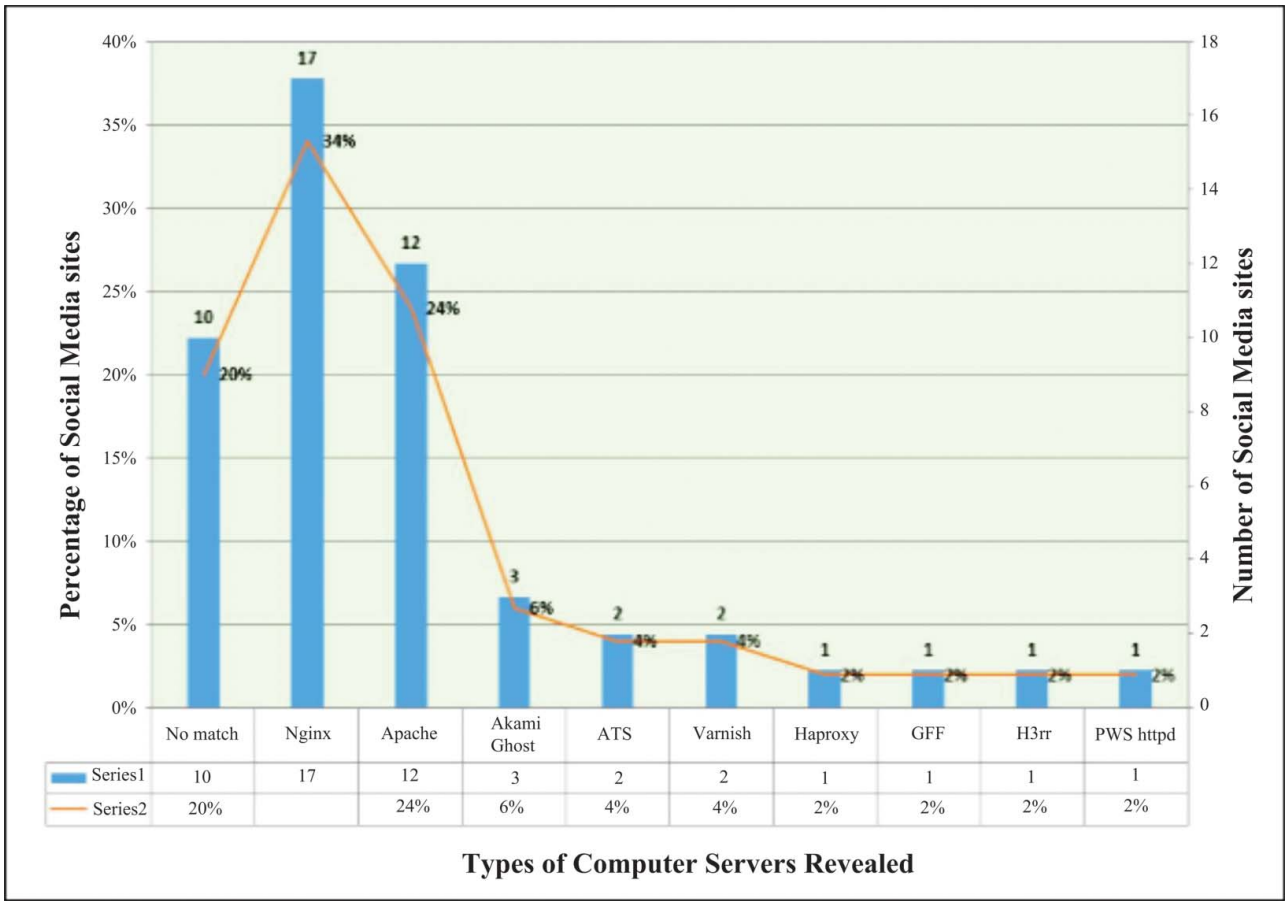

FIGURE 5. Server systems vulnerability status of social media sites.

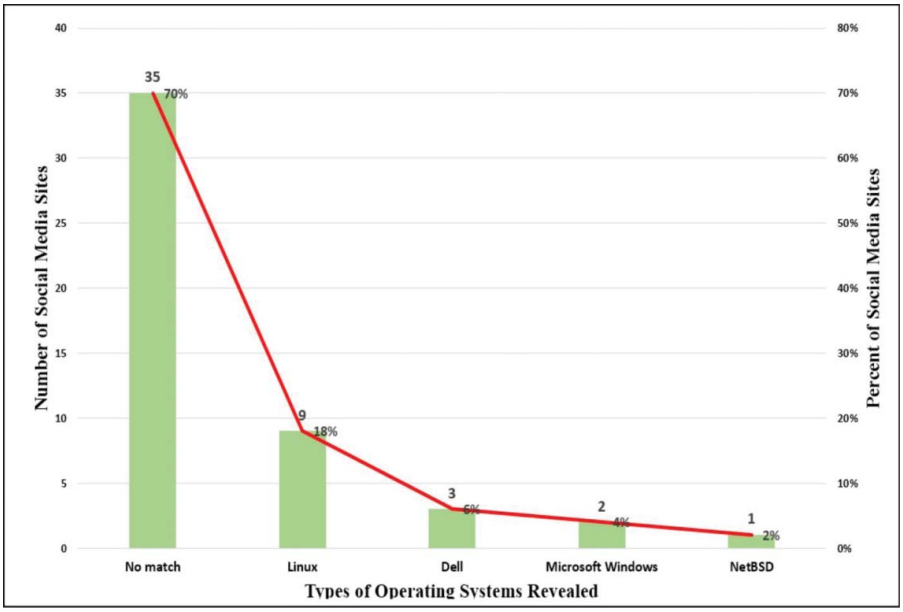

FIGURE 6. Operating systems vulnerability status of social media sites.

TABLE 4
Independent *t*-Test of Security Measures Between U.S.-Based and Other Country-Based Social Media Sites

Security measures	Country base: 1 = United States; 2 = other	*n*	*M*	*SD*	*t*	*df*	Sig. (two-tailed)
Child protection policy present on social networking site	1	35	1.000	0.000	4.099	48	.000*
	2	15	0.667	0.488			
Privacy policy present on social networking site	1	35	1.000	0.000	3.495	48	.001*
	2	15	0.733	0.458			
SSL encryption	1	35	0.800	0.406	2.961	48	.005*
	2	15	0.400	0.507			
Security policy present on social networking site	1	35	0.914	0.284	2.802	48	.007*
	2	15	0.600	0.507			
Proper use statement present on social networking site	1	35	0.914	0.284	2.802	48	.007*
	2	15	0.600	0.507			
No liability statement present on social networking site	1	35	0.971	0.169	2.705	48	.009*
	2	15	0.733	0.458			

*$p < .01$.

the site's security measures, but also to deter potential intruders and attackers from trying improper activities (Ashford, 2014b; Symantec, 2015).

Second, the majority of the social media sites' network information was publicly available through the Google search. Such information included networks' IP address and physical address; network range, name, handle, type, parent, and CIDR; registration date, last updated time, phone number, and email address. The information makes the sites vulnerable to cyber intrusions and attacks. For example, searching for the IP address of a site is often the first step for cyber intruders to connect to the server of the site. In addition, the network range and CIDR address reveal the total number of hosts the network possess and the network's higher and lower level routing information. Having put these pieces of information together, a cyber intruder has a full picture of which parts of the network are vulnerable and easy to intrude. These findings suggest that social media sites should consider negotiating with American Registry of Internet Numbers on requiring username and password login for access to a web portal's registration information. To make the negotiation successful, social media companies need to form an industry alliance and conduct collective negotiation with American Registry of Internet Numbers.

Furthermore, the network scan illustrated that the social media sites had most of their ports closed, filtered, or behind firewalls; only very few ports were detected as open: Port 80/TCP and Port 443/TCP. The open Port 80/TCP enabled Nmap to detect that 80% of the sites were running servers such as Nginx (34%), Apache (24%), AkamaiGHost (6%), ATS (4%), Varnish (4%), Haproxy (2%), GFE (2%), H3rr (2%), and PWS httpd (2%). Obviously, the sites currently keeping open Port 80/tcp should consider adopting more secured open Port 8080/tcp for http-proxy, thereby making the site anonymous on the Internet. Regarding the open Port 443/TCP or alternative Port 8443/TCP for encrypted https services, user IDs and passwords must be required to grant access to the port and outgoing access to the port from servers should be restricted.

Finally, the U.S.-based social media sites had significantly more policies and measures than other country-based counterparts in the following six aspects: privacy policy, security policy, child-protection policy, SSL encryption, proper use statement, and no-liability statement. Therefore, other country-based social media sites should consider following the U.S. examples regarding such policies and measures.

RECOMMENDATION FOR FURTHER RESEARCH

We recommend that a further study of this type be conducted in three years among the active social media sites around the world for measuring their site security and vulnerability, comparing the sites for strengths and weaknesses, and identifying opportunities for further improvement.

REFERENCES

Ashford, W. (2014a). Google could face $100 million lawsuit over nude celebrity pictures. *Computer Weekly*. Retrieved from http://www.computerweekly.com/news/2240232039/Google-could-face-100m-lawsuit-over-nude-celebrity-pics

Ashford, W. (2014b). Social media threats to business on the rise. *Computer Weekly*. Retrieved from http://www.computerweekly.com/news/2240236398/Social-media-threats-to-business-on-the-rise-says-report

Berthon, P. R., Pitt, L. F., McCarthy, I., & Kates, S. (2007). When customers get clever: Managerial approaches to dealing with creative consumers. *Business Horizons*, *50*, 39–48.

Boggs, R. A., & Walters, D. (2006). A longitudinal look at e-government in practice. *Issues in Information Systems*, *7*, 161–164.

Bureau of Labor Statistics. (2014). *The 2014 occupational outlook handbook*. Retrieved from http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

Campbell, D., & Beck, A. C. (2004). Answering allegations: The use of the corporate website for restorative ethical and social disclosure, *Business Ethics*, *13*, 100.

Cavaliere, V. (2012). Hasbro Easy-Bake Oven to be marketed to girls and boys in 2012 following petition for change by 13-year-old girl. *New York Daily News*. Retrieved from http://www.nydailynews.com/new-york/hasbro-easy-bake-oven-girls-boys-article-1.1222592

Garcia, R. C. (2004). Network security: Mapping intrusion and anomaly detection to very-high-degree polynomials. *Signals, Systems, and Computers*, *2*, 1449–1452.

Gay, R. (2014). The great 2014 celebrity nude photos leak is only the beginning. *The Guardian*. Retrieved from http://www.theguardian.com/commentisfree/2014/sep/01/celebrity-naked-photo-leak-2014-nude-women

Jamieson, S. (2002). *The ethics and legality of port scanning*. Bethesda, MD: SANS Institute. Retrieved from http://www.sans.org/reading_room/whitepapers/legal/the_ethics_and_legality_of_port_scanning_71?show=71.php&cat=legal

Kietzmann, J. H., Hermkens, K., McCarthy, I. P., & Silvestre, B. S. (2011). Social media? Get serious! Understanding the functional building blocks of social media. *Business Horizons*, *54*, 241–251.

McNurlin, B. C., & Sprague, R. H. Jr. (2006). *Information systems management in practice* (7th ed.). Upper Saddle River, NJ: Pearson Prentice Hall.

Moorman, C. (2012). *Social media spend continues to soar*. Durham, NC: The CMO Survey. Retrieved from http://www.cmosurvey.org/blog/social-media-spend-continues-to-soar/

Nerney, C. (2011). 5 top social media security threats. *Network World*. Retrieved from http://www.networkworld.com/article/2177520/collaboration-social/5-top-social-media-security-threats.html

Symantec. (2015). *2015 Internet security threat report*. Retrieved from http://www.symantec.com/security_response/publications/threatreport.jsp?inid=us_ghp_hero1_istr20

Trustwave. (2015). *The 2015 trustwave global security report*. Retrieved from https://www2.trustwave.com/rs/815-RFM-693/images/2015_TrustwaveGlobalSecurityReport.pdf

U.S. Department of Justice. (2003). Fraud and related activity in connection with computers. In *United States Code Annotated* (Title 18, Chapter 47, Section 1030). Washington, DC: Author. Retrieved from http://www.usdoj.gov/criminal/cybercrime/1030NEW.htm

Wilkinson, V. O. & Cappel, J. J. (2005). Impact of economic prosperity and population on e-government involvement. *Issues in Information Systems, 6*, 204–209.

Winkler, I. (2004), What is a security audit? *Tech Target*. Retrieved from http://searchcio.techtarget.com/sDefinition/0,,sid182_gci955099,00.html

Zhao, J. J., Truell, A. D., Alexander, M. W., & Davis, R. (2006). State e-government service and economic competitiveness: A relational analysis. *Issues in Information Systems*, *7*, 171–176.

Zhao, J. J., & Zhao, S. Y. (2004). Internet technologies used by INC. 500 corporate web sites. *Issues in Information Systems*, *5*, 366–372.

Zhao, J. J., & Zhao, S. Y. (2014). The impact of corporate social media on revenue and profit: An exploratory study. *International Journal of Management and Information Technology*, *10*, 1892–1902.