IST-Africa 2018 Conference Proceedings
Paul Cunningham and Miriam Cunningham (Eds)
IIMC International Information Management Corporation, 2018
ISBN: 978-1-905824-60-1

Major Security Incidents since 2014: an African Perspective

Renier VAN HEERDEN[1,2], Sune VON SOLMS[3] Johannes VORSTER[4]
[1]*Meraka Institute, Council for Scientific and Industrial Research, Brummeria, Pretoria, South Africa*
Tel: +27 12 841 3434, Fax: +27 12 841 2455, renier@sanren.ac.za
[2]*Department of Information Technology, Nelson Mandela University, Port Elizabeth, South Africa*
[3]*University of Johannesburg, Department of Electrical and Electronic Engineering Science,*
Faculty of Engineering and the Built Environment, Johannesburg, South Africa
Tel: +27 11 559 2462, Email: svonsolms@uj.ac.za
[4]*Rhodes University, Department of Computer Science, Grahamstown, South Africa*
Tel +27 46 603 829, compsci@ru.ac.za

Abstract: The integration of technology in the modern society provides many benefits, but with increased connectivity comes increased risk where governments, businesses and individuals are vulnerable to a variety of cyber-attacks. Many of the large information security attacks of the last decade can be seen as an attack on 'foreign" systems or individuals when viewed from an African perspective, with no direct impact on an individual in Africa. However, information security experts in Africa states that although some of these attacks might not have had a direct impact of the African individual, but never the less should not be ignored as it does indirectly influence the African individual. The experts state that even if the individuals or businesses are not directly influenced by an attack, it should not be ignored as similar attacks might influence them in the future. They emphasise that these attacks should improve their cybersecurity awareness and behaviour, in order to prevent similar attacks from impacting them.

Keywords: Information security, cyber-attacks, Africa

1. Introduction

The impact that technology on modern society can clearly be seen by the development of technologies such as the iPhone [1]. Facebook, the largest social media platform in the world, has nearly 2 billion users worldwide [2] and the Internet of Things (IoT) is predicted to have more than 6 billion connected devices by 2020 [3]. The integration of technology in the modern society provides many benefits, but this connectivity has also made governments, businesses and individuals vulnerable to cybercrimes, such as identity theft, fraud and espionage. IBM CEO stated that "Cybercrime may be the greatest threat to every company in the world," and reported that 2015 saw 1.5 million cyber-attacks [4], which included breached home automation systems, hacked factory floors or stolen electronic health records, which can be catastrophic for individuals as well as for manufacturers.

The rate of Africa's internet growth is the highest globally, where the bandwidth growth is 51% over the last five years [5]. The Global Internet Geography report states that "growth in international internet capacity connected to Africa continues to outpace that of any other region" [6]. Unfortunately, the increasing technological exposure of African poses its own vulnerabilities and risk. With the rise in cybercrime globally, the cybercrime in Africa is increasing at a more rapid rate than anywhere else in the world [7].

Many of the massive information security incidents of the past decade is on a global scale, where the attack on an operating system or global brand has a direct impact on an individual in Africa. However, due to the connected nature of individuals globally, information security attacks which may be considered as "foreign" (attacks on a bank, server or online store elsewhere) may have an indirect impact on the African individual as well. This paper aims to discuss the top information security incidents from 2014 and evaluate the impact of these attacks on the African individual. The paper contains the collected opinions of information security experts in Africa on the impact of information security breaches on the African individual.

2. Information Security Attacks and the African Landscape

In the Enterprise Security Risks and Workforce Competencies survey in 2015, professionals named cybersecurity as the number one risk that enterprises are likely to face in the upcoming years [8]. This is evident in the cyber-attacks in the last decade and especially lately. In 2014 security researchers found a bug in software used by major companies, including Google, Amazon and the US government. The Heartbleed bug was a security vulnerability which compromised security, which allowed attackers to intercept sensitive personal data, eavesdrop on communications and to impersonate services and users. [9, 10]. Within the same year, a 22 year old security bug, named Shellshock, was discovered which affected most versions of the Linux and Unix operating systems which is estimated to be up to 70% of machines connected to the. The successful exploitation of Shellshock could allow an attacker to gain access and control of an infected computer and potentially the network it is connected to Internet [11]. 2017 has seen the massive WannaCry ransomware attack, which targeted machines by exploiting vulnerabilities in Windows computers which were not updated with the latest Microsoft security patches [12,13].

IoT is predicted to have more than 6 billion connected devices by 2020 [3], including automated devices in the home, factory floors and even self-driving cars. These devices, on top of the traditional computer infrastructure can be targeted by cyber criminals if not properly secured. A 2015 Veracode study which evaluated the security of 6 major home automation systems found major security flaws in 5 of them [14]. The results of the study stated the designers of the tested devices "weren't focused enough on security and privacy, as a priority, putting consumers at risk for an attack or physical intrusion". Poorly build integrated systems can have a major impact on the individuals and businesses who use them as well as the manufacturers [4]. Dan Gardner, Principal Analyst at Interarbor Solutions said in an interview that vulnerability increases with connection, meaning that the more physical things are connected to the Internet, the higher the prospect for criminals to exploit possible security flaws [15].

Cybercrime, including identity theft, fraud and espionage, is a growing global phenomenon with the highest growing rate in Africa [16]. Statistics from various security reports indicate that Africa is prone to cyber-threats as a high number of domains are coupled with very weak network and information security [7]. It is estimated that cybercrimes cost the African economy approximately $895 million annually [17] and that South Africa has the third highest number of cybercrime victims in the world [18]. In the light of these statistics, however, Africa still has a lack of technical know-how in terms of cybersecurity, which includes the ability to monitor and defend national networks, as well as lacking cybersecurity legal frameworks to fight cybercrime. Africa also lacks significant cybersecurity initiatives and limited levels of security awareness, where organisations are ill prepared to deal with information security threats due to a lack of knowledge, funding and skilled professionals [7, 17].

Due to the connected nature of today's individual, every individual is a potential target. In many cases, cybercriminals target the end user, as they are potentially the easiest at which the criminal can gain access to the individual's information or a company's systems [19]. However, individuals generally struggle to understand the impact of large information security incidents if they are not directly targeted, for example by a social engineering scam or financial crime where money was stolen. A famous case was when Aaron Barr believed he had penetrated Anonymous (international hacking and free information group)[40]. Even though Aaron was familiar with information security, Anonymous had managed to infiltrate Aaron Barr company official website and replace it with a pro-Anonymous message: "now the Anonymous hand is bitch-slapping you in the face." They also got into HBGary government e-mail server, for which Barr was the administrator, and compromised it, extracting over 40,000 e-mails and putting them up on the web. [40]

3. Methodology

This paper relied on a number of research avenues, including a security survey completed by information security experts in South Africa; extensive reviews of global security reports; and the authors' analysis of the body of research conducted by others on the topic of cybersecurity.

In connection with the conducted security survey, respondents were information security experts from various academic and government institutions across South Africa. The survey consisted of closed- and open ended questions, which included the following:

1. A collection of some of the top information security incidents since 2014 is provided. Rank the top 3 incidents according to you and the impact that it had on you as a security specialist.
2. Rank the top 3 incidents considering the impact on Africa and the African individual.
3. Motivate the selections made.
4. Considering the information security incidents discussed above, what would you say is the top information security threat for Africa in the future?

This paper goal is not to provide a definitive answer to the question of how major security incidents since 2014 affected African but rather a starting point from which an African understanding of perspective of major security incidents.

4. Technology Description

In this section we give an overview of the most significant security incidents. This paper goal is not to go into detail of each incident, but rather give a quick overview. The incidents discussed in this section are the incidents identified by the researchers as the top major global security incidents since 2014. These incidents were included in the Information Security Survey discussed in Section 4.

4.1 Meltdown and Spectre

Early in 2018, the Meltdown and Spectre exploit exploited serious vulnerabilities in computer processors. These vulnerabilities allowed programs to steal data while being processed. Meltdown and Spectre work on personal computers, mobile devices and in the cloud [20] where it aimed to get hold of confidential data stored in the memory of separate running programs. Possible vulnerable data could include passwords stored in a password manager or browser and even confidential documents. Meltdown overcome the most central isolation between user applications and the operating system where Spectre breaks the isolation between different applications. Peter Bright states that: "all modern processors, including those from Intel, AMD, and ARM" are affected by Meltdown". [21]

4.2 WannaCry

The WannaCry ransomware attack in 2017 was a worldwide cyberattack by the WannaCry ransomware cryptoworm, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency. WannaCry Ransomware is malicious software that blocks user access to files or systems, keeping files or complete devices hostage using encryption until the victim pays a ransom in exchange for a decryption key, which allows the user to access the files or systems encrypted by the program [22].

4.3 200 million US Voter Records Exposed

In 2017, various databases containing nearly 200 million records on United States voters from various political parties were found stored on an open Amazon storage server owned by a Republican data analytics firm, Deep Root Analytics [23]. Zack Whittaker from ZDNET believed it to be the largest ever known exposure of voter information up to 2017. Record listing a voter's name, date of birth, home address, phone number, and voter registration details as to which political party a person is registered with was leaked. [23]

4.4 Gmail Users were Targeted in a Sophisticated Phishing Scam

Gmail users were targeted in a sophisticated phishing scam that was seeking to gain access to accounts through a third-party app in 2017. In about one hour and the company says they estimate about 1 million users may have been affected [24].

4.5 South Africans' Personal Info Exposed

The largest data leak recorded in South Africa has been traced to an open web server in 2017. The breach contains data of more than 30-million unique South African identity (ID) numbers, address, income, living standard measure, contact numbers and employment information. Security researcher Troy Hunt discovered a leaked database is a 27.2GB backup file that stored over 47 million records [25].

4.6 Old breaches shake LinkedIn, Tumblr, VK and DropBox:

Cybercriminal going by the name of ‘Peace’ came to prominence in 2016 after data on millions of LinkedIn, Tumblr and Myspace users was made available online. In total there were more than half a billion passwords posted and an estimated 500 million credentials were stolen. Table 1 contains the sites which were breached and data stolen, according to Andrew Komarov [26].

Table 1: Breached sites and number of stolen records

Breach company	Number of records
Yahoo!	500 million (up to 1bn)
Myspace	360 million
LinkedIn	167 million
Vk.com	137 million
Qip.ru	133 million
Badoo	126 million
Dropbox	103 million (Dropbox cites a breach of 68 million due to password reuse)
Rambler.ru	101 million

Tumblr	50 million
LastFM	43 million
Fling.com	40 million
Mobango.com	6 million

4.7 YAHOO Data Breach

In 2016 Yahoo announced that half a billion of its accounts had been hacked, where security experts discovered that Yahoo suffered the breached in 2012 and 2014 [27]. Names, email addresses and passwords were disclosed. Yahoo used an older MD5 algorithm to hash their password which gave hackers an opportunity to get account data. Also, Yahoo servers were compromised in 2013 where security questions and answers were compromised.

4.8 Democratic National Committee (USA) Leak

A collection of over 19,000 emails from the Democratic National Committee (DNC), the governing body of the Democratic Party of the United States, was leaked and published by WikiLeaks in 2016. Although speculative, these leaked emails could have influenced the election between Hilary Clinton and Donald Trump enough to change the final result [28]. What make this leak more interesting is that currently it is speculated that the hacker who stole the data was sponsored by the Russian state [29].

4.9 "Weaponizing" the Internet of Things – The DYN DNS Hack

A massive distributed denial of service (DDoS) attacks powered by Internet of Things devices created serious problems in 2016 [30]. The attack targeted websites and services, such as Twitter, GitHub, PayPal, Amazon, Reddit, Netflix, and Spotify. Hackers used open source code to build a botnet army of Internet of Things devices, and then directed those devices to send massive waves of junk requests to a DNS provider. The compromised Internet of Things devices, which make up the bot-net army, are still out there and unpatched, thus Jeff Roberts speculates that other attacks are likely on the way [31].

4.10 Ashley Madison Data Theft

The Impact Team hacker group accessed the Ashley Madison user database in 2015, revealing financial records and other proprietary information, including the personal data of 37 million users. Ashley Madison is a dating website for people looking for extra-marital relationships, with the slogan: Life is short, have an affair. Essentially, the hackers' foremost motivation were that they consider the Ashley Madison site to be deceitful. Their main grievance was with Ashley Madison's full delete service which did not in reality delete the users data [32].

4.11 Anthem Health Care Hack

The second-largest health insurer in the USA, Anthem Health Care, estimated approximately 78.8 million highly-sensitive patient records were breached, that quickly increased to an additional 8.8 to 18.8 million non-patient records. The hack was noticed in 2015 when employees of Anthem noticed unusual database queries. In retrospect, the main fault of Athhem was not to encrypt their data. The hackers were able to steal the following information [33]:

- Full Names

- Physical addresses
- Email addresses
- Social Security numbers
- Birthdates
- Insurance membership numbers
- Medical IDs
- Employment information
- Income data

4.12 Hackers Figured Out How to Remotely Take Control of Jeep Cherokee

Chrysler recalled 1.4 million vehicles in 2015 possibly affected by the vulnerability the researchers found in the Jeep's UConnect infotainment system that allowed them to hijack its steering, braking, and accelerator, among other things. One vulnerable element, which Miller and Valasek have identified at Black Hat talk, lets anyone who knows the car's IP address gain access from anywhere in the country. The hack moves from the hardware for its entertainment system to the controlling firmware. That changed firmware is used to send commands to the car's internal computer network via CAN bus thus effecting physical components like the engine and wheels [34].

4.13 A Billion Android Devices Compromised by Vulnerability in the Operating System

These exploits was discovered in 2015 and let hackers take over the operating system of any Android phone without the user even knowing. With almost 1 billion Android devices affected, security researchers were quick to call it one of the biggest smartphone security flaws ever. Six dangerous vulnerabilities have left over 95% of Google Android phones open to an attack delivered by a multimedia texts. In worst cases, the smart phones parse the attack code before to the message is opened, thus the attack is silent and without the user capable of defending against it [35].

4.14 JP Morgan & Chase Cyber-Attack Data Breach

JP Morgan & Chase was struck with a brutal cyber-attack, leading to the loss of data belonging to 76 million households and 7 million businesses. The hackers have obtained the list of the software that run on JPMorgan’s computers, which they used to find known vulnerabilities, thus searching of an entry point back into the bank’s systems. The hackers gained access to the names, addresses, phone numbers and emails of JPMorgan account holders [36].

4.15 Sony Pictures Targeted by Protest Hackers (2014)

Sony found itself targeted by a group of hackers which stole and released films in production and leaked company emails. A group of hackers known as Guardians of Peace (GoP), posted internal salary information from Sony Pictures online they had apparently stolen in their attack. It is speculated that GoP were backed by the North Korean government and the hack was in retaliation for Sony Pictures showing the film The Interview, a fictional comedy in which two journalists try to assassinate North Korean leader Kim Jong Un on behalf of the CIA. Kim Jong Un has condemned the movie as “an act of war.” [37]

4.16 Heartbleed

The Heartbleed Bug, discovered in 2014, is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet [10]. The Heartbleed security bug allows anyone on the Internet to access the memory of the systems protected OpenSSL software. This negates the secret keys used to identify the data providers and to encrypt the traffic, the usernames and passwords of the users and the actual data. This attack allowed eavesdropping on communications, stealing of data and malicious users and to impersonate valid users [38].

4.17 ShellShock

A 2014 vulnerability that affected most versions of the Linux and Unix operating systems, in addition to Mac OS X (which is based around Unix). This vulnerability could allow an attacker to gain control over a targeted computer if exploited successfully. The vulnerability affects BASH, a common component known as a shell that appears in nearly all versions Unix 9and thus Linux) which acts as a command language interpreter. This allowed users to type commands into a text-based environment, which the operating system will then execute. BASH can also be used to execute commands passed to it by applications and it is this feature that the vulnerability affects [11]. A command that can be sent to Bash permits environment variables to be allocated. The vulnerability used in the circumstance is that an attacker can add malicious code to the environment variable, which will run once the variable is received.

5. Results

This section discusses the results of the survey conducted relating to the impact of information security incidents on African individuals.

The first collection of questions required the expert to state which of the incidents, discussed in section 3, had the biggest impact on them personally. The results of this question is summarised in Figure 1. Note that the experts were required to select their top 3 incidents, so the provided percentages sums to 300%.

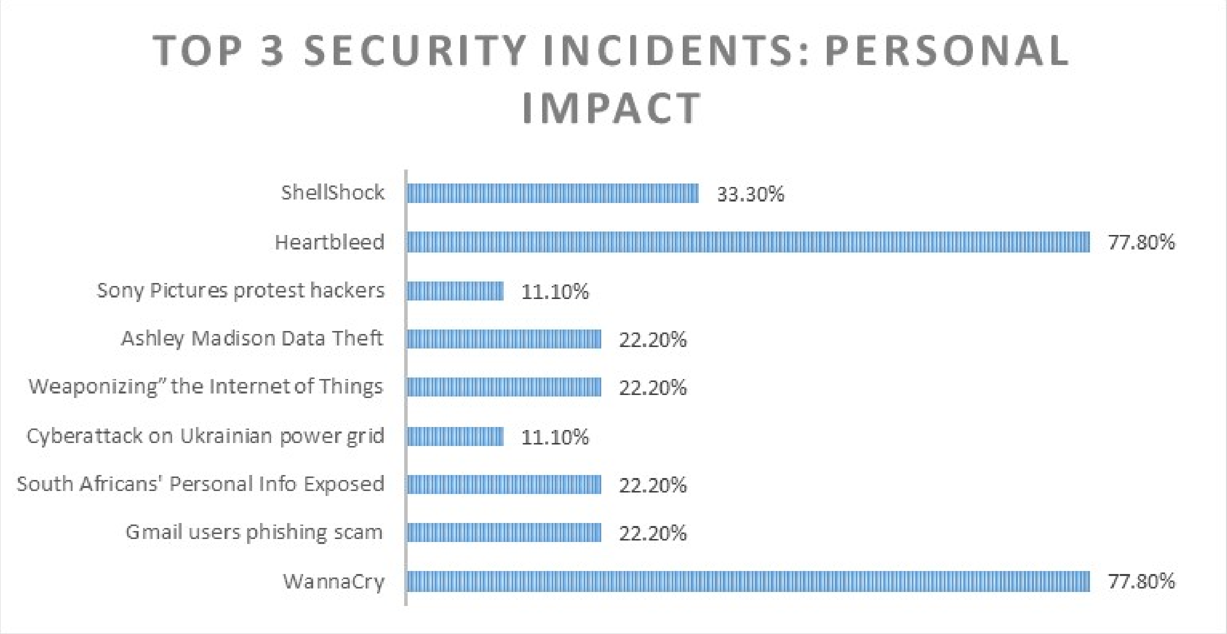

Figure 1: Top 3 security incidents-personal impact

Providing examples of incidences where some of these attacks directly affected the experts, one expert stated that the WannaCry attack required him to "assist in managing a customer's patching mechanism". Another respondent stated that "Ransomware probably had the highest impact". A respondent stated that the Heartbleed bug "created a number of difficulties in reconfiguring secure sites to ensure only the latest algorithms were used". These attacks were the highest rated attacks by the experts as shown in Figure 1.

Referring to the more general impact of the attacks, a respondent stated that "South Africa has now become a target" and that many of the top information security incidents targets data, which "shows that within the context of South Africa that security needs to be improved". The exposure of South Africans' personal information was one of the examples sighted as well as the example of the Ashley Madison data theft.

The same incidents were again presented to the respondents and they were required to rate the top 3 incidents as they impacted Africa and the African individuals. The results obtained are shown below in Figure 2:

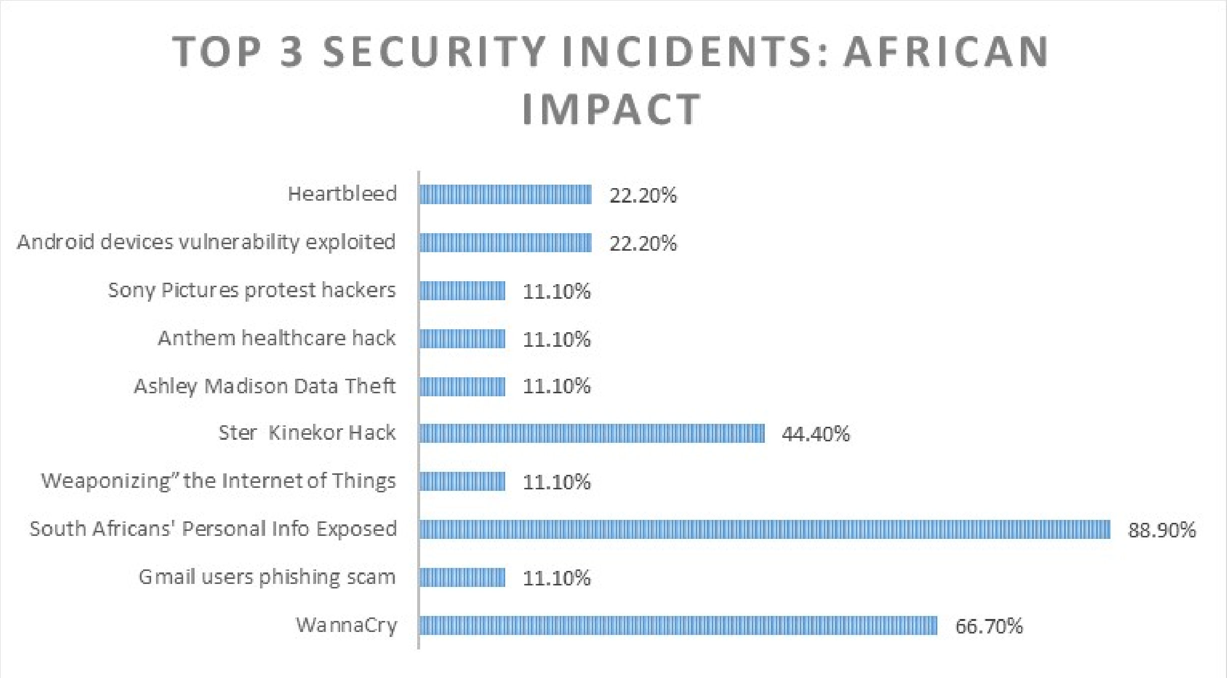

Figure 2: Top 3 security incidents-African impact

Two of the highest rated incidents directly affected South Africans as the data of South African individuals were exposed (Ster Kinekor hack and the exposure of South Africans' personal information). The experts stated that many of the incidents might not have affected African individuals directly, but hope that these incidents help to increase the awareness and attention around information security. One experts mentioned that these data breaches of South Africans' personal information have "shown the lack of implementation (of the POPI Act) and the impact of current cyber security solution as implemented in South Africa is not working". The Protection of Personal Information Act 4 of 2013 (POPI Act) promotes the protection of personal information by public and private bodies. It has been signed into law in 2013 and effective from 2014 [39].

The experts placed great emphasis on Internet of Things (IoT) and embedded systems as a new avenue for information security incidents. One expert writes that "a new attack vector, IoT, is under development which will affect the field of ICT in the long term". Another further states that "DDoS impact from IOT was wide spread in terms of impact and risk".

Lastly, the experts were asked what they would say is the top information security threat for Africa in the future. The experts continued on the main topics mentioned in the previous questions relating to personal information disclosure and data breaches mainly due to the exploitation of unpatched systems and poorly secured systems holding Personal Identifiable Information (PII). They continue to comment on the fact that many companies and corporations are “not always placing enough emphasis on securely storing and managing sensitive and private information”. They mention the potential value which can be gained by cyber criminals in using the collected data to conduct further attacks or to sell the personal information.

Experts also mentioned the “lack of relevant cyber education and awareness” and the utilisation of social engineering to exploit individuals. Cyberattacks on financial institutions and cyber-attacks on national critical infrastructure are also named as a possible future threat as well as the infection with cryto-currency miners.

6. Conclusions

The connected nature of individuals and businesses in Africa makes everybody a potential target for a cyber-attack. Information security incidents are frequently discussed in the news and through various media avenues. In most cases, the incidents which African individuals hear about is of a global nature which seem not to influence them directly, and they struggle to understand the impact of these incidents if they are not directly targeted. This paper discussed the top information security incidents from 2014 and evaluated the impact of these attacks on the African individual. The collected opinions of information security experts in Africa provided their insights on the impact of information security breaches on the African individual.

Results from a survey to information security experts state that personal information disclosure due to the exploitation of unpatched and poorly secured systems holding PII is a major threat for African individuals. The lack of cyber security awareness is also sighted as a threat to individuals. The experts state that even if the individuals or businesses are not directly influence by an attack, it should not be ignored as similar attacks might influence them in the future. Therefore they should be vigilant and improve their behaviour, storage mechanisms or management of PII to prevent similar attacks from impacting them.

The question for following up from this research will be how to reduce key risk factors and recommendations for individuals, organisations and governments with an African perspective. The main implication for Africa is that it will also be at risk from information security incidents and thus should also prepare to mitigate against it.

References

[1] D.E. Dilger, “Ten Years of iPhone: the past present and future of Apple's blockbuster phenomenon,” appleinsider, January 2017. Available at: http://appleinsider.com/articles/17/01/09/ten-years-of-iphone-the-past-present-and-future-of-apples-blockbuster-phenomenon- Accessed January 2018.

[2] D. Noyes, “The Top 20 Valuable Facebook Statistics – Updated January 2018”, January 2018. Available at: https://zephoria.com/top-15-valuable-facebook-statistics/ Accessed January 2018.

[3] A. Nordrum, “Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated”, IEEE Spectrum, 2016. Available at: https://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated Accessed January 2018.

[4] S. Margan, “IBM's CEO On Hackers: 'Cyber Crime Is The Greatest Threat To Every Company In The World'”, Forbes, November 2015. Available at: https://www.forbes.com/sites/stevemorgan/2015/11/24/ibms-ceo-on-hackers-cyber-crime-is-the-greatest-threat-to-every-company-in-the-world/#6a2d1cba73f0 Accessed January 2018.

[5] T. Shapshak, “African Internet Growth Continues To Outstrip The World”, Forbes, September 2015. Available at: https://www.forbes.com/sites/tobyshapshak/2015/09/02/african-internet-capacity-growth-continues-to-outstrip-the-world-2/#ae3e327568ed Accessed January 2018.

[6] TeleGeography, “Africa’s international bandwidth growth to lead the world”, 2013. Avaialble at: https://www.telegeography.com/products/commsupdate/articles/2013/10/31/africas-international-bandwidth-growth-to-lead-the-world/ Accessed August 2017.

[7] United Nations Economic Commission for Africa, “Tackling the challenges of cybersecurity in Africa”, United Nations, 2014. Available at: https://www.uneca.org/sites/default/files/PublicationFiles/ ntis_policy_brief_1.pdf Accessed January 2018.

[8] University of Phoenix, “Competency Models for Enterprise Security and Cybersecurity Research”, 2015.

[9] R. Nieva, “Heartbleed bug: What you need to know (FAQ)”, CNET, April 2014. Available at: https://www.cnet.com/news/heartbleed-bug-what-you-need-to-know-faq/ Accessed January 2018.

[10] Heartbleed information site, “The Heartbleed Bug”, 2017. Available at: http://heartbleed.com Accessed January 2018.

[11] Symentec, “Shellshock Vulnerability”, Symentec, 2017. Available at: https://www.symantec.com/outbreak/?id=shellshock Accessed January 2018.

[12] T. Warren, “Microsoft issues ‘highly unusual’ Windows XP patch to prevent massive ransomware attack", The Verge, May 2017. Available at: https://www.theverge.com/2017/5/13/15635006/ microsoft-windows-xp-security-patch-wannacry-ransomware-attack Accessed May 2017.

[13] Symantec Security Response, “What you need to know about the WannaCry Ransomware”, Symantec, October 2017. Available at: https://www.symantec.com/connect/blogs/what-you-need-know-about-wannacry-ransomware Accessed January 2018.

[14] Veracode, “The Internet of Things: Security Research Study”, White Paper, 2014. Available at: https://www.veracode.com/sites/default/files/Resources/Whitepapers/internet-of-things-whitepaper.pdf Accessed August 2017.

[15] D. Gardner, “Capgemini and HPE Team Up to Foster Behavioral Change That Brings Better Cyber Security Across Application Lifecycles”, Interarbor Solutions, April 2016. Available at: http://www.briefingsdirecttranscriptsblogs.com/2016/04/capgemini-and-hpe-team-up-to-foster.html Accessed August 2017.

[16] Symantec Corporation, “Internet Security Threat Report 2013, 2012 Trends”, Volume 18, April, 2013. Available from www.symantec.com/content/ en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.enus.pdf. Accessed January 2018.

[17] P. Musuva-Kigen, F. Mueni, D. Ndegwa et.al. “Africa Cyber Security Report 2016”, Serianu Cyber Threat Intelligence Team, 2016.

[18] Symantec Corporation, 2012 Norton Cybercrime Report, September 2012.

[19] Business Media, “SA Ranks World’s Third Highest Cybercrime Victims”, Business Media, 2017. Available at: http://businessmediamags.co.za/sa-ranks-worlds-third-highest-cybercrime-victims-2/ Accessed January 2018.

[20] Graz University of Technology, “Meltdown and Spectre”, 2018. Available at: https://meltdownattack.com/ Accessed January 2018.

[21] P. Bright, “’Meltdown’ and ‘Spectre’: Every modern processor has unfixable security flaws”, January 2018. Available at: https://arstechnica.com/gadgets/2018/01/meltdown-and-spectre-every-modern-processor-has-unfixable-security-flaws Accessed January 2018.

[22] A. Hern and S. Gibbs, “What is WannaCry ransomware and why is it attacking global computers”, The Guardian, May 2017.

[23] Z. Whittaker, “198 million Americans hit by 'largest ever' voter records leak”, ZDNet, 2017. Available at: http://www.zdnet.com/article/security-lapse-exposes-198-million-united-states-voter-records/ Accessed January 2018.

[24] S. Levin, “Google Docs users hit with sophisticated phishing attack in their inboxes”, The Guardian, May 2017. Available at: https://www.theguardian.com/technology/2017/may/03/google-docs-phishing-attack-malware Accessed January 2018.

[25] MyBroadband, “Private data of 30 million South Africans exposed in massive leak”, BusinessTech, October 2017. Available at: https://businesstech.co.za/news/internet/205730/30-million-south-africans-exposed-in-massive-data-leak/ Accessed January 2018.

[26] D. Pauli, “Security analyst says Yahoo!, Dropbox, LinkedIn, Tumblr all popped by same gang • The Register”, September 2016. Available at: https://www.theregister.co.uk/2016/09/30/ fiveperson_hacking_gang_claimed_behind_ breaches_of_3bn_logins/ Accessed January 2018.

[27] S. Larson, “Every single Yahoo account was hacked - 3 billion in all”, CNN Tech, October 2017. Available at: http://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html Accessed January 2018.

[28] H. Enten, “How Much Did WikiLeaks Hurt Hillary Clinton?“, FiveThirtyEight, 2016. Available at: https://fivethirtyeight.com/features/wikileaks-hillary-clinton/ Accessed January 2018.

[29] G. Smith, “A Russian Hacker Confessed to Hacking the DNC During the Election Campaign”, Fortune, December 2017. Available at: http://fortune.com/2017/12/11/russian-hacking-election-confession/ Accessed January 2018.

[30] M. Kumar, “An Army of Million Hacked IoT Devices Almost Broke the Internet Today”, The Hacker News, October 2016. Available at: https://thehackernews.com/2016/10/iot-dyn-ddos-attack.html Accessed January 2018.

[31] J.J. Roberts, “Who to Blame for the Attack on the Internet”, October 2016. Available at: http://fortune.com/2016/10/23/internet-attack-perpetrator/ Accessed January 2018.

[32] S. Mansfield-Devine, “The Ashley Madison affair”, Network Security, No 9, pp 8-16, 2015.

[33] C. Sienko, “The Breach of Anthem Health - the Largest Healthcare Breach in History”, Infosec Institute, 2015. Available at: http://resources.infosecinstitute.com/category/healthcare-information-security/healthcare-attack-statistics-and-case-studies/case-study-health-insurer-anthem/#gref Accessed January 2018.

[34] A. Greenberg, “Hackers Remotely Kill a Jeep on the Highway—With Me in It”, Wired, July 2015. Available at: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ Accessed January 2018.

[35] T. Fox-Brewster, “Stagefright: It Only Takes One Text To Hack 950 Million Android Phones”, Forbes, July 2015. Available at: https://www.forbes.com/sites/thomasbrewster/2015/07/27/android-text-attacks/#6fa030dd3a50 Accessed January 2018.

[36] J. Silver-Greenberg, M. Goldstein and N. Perlroth, “Discover all that The Times has to offer”, The New York Times, October 2014. Available at: https://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/ Accessed January 2018.

[37] T. Huddleston Jr., “What you need to know after Sony's hacker attack”, Fortune, December 2014. Available at: http://fortune.com/2014/12/03/need-to-know-cyber-attacks/ Accessed January 2018.

[38] S. Gujrathi, “Heartbleed bug: AnOpenSSL heartbeat vulnerability”, International Journal of Computer Science and Engine ter Science and Engineering, Vol 2, No 5, pp 61-64, 2014.

[39] SAICA, “Protection of Personal Information Act”, SAICA, September 2017. Available at: https://www.saica.co.za/Technical/LegalandGovernance/Legislation/ProtectionofPersonalInformationAct/tabid/3335/language/en-ZA/Default.aspx Accessed January 2018.

[40] G. Coleman, 2013. “Anonymous in context: The politics and power behind the mask”, Internet Governance, Vol 3, pp 1—27, 2013