Advances In Multidisciplinary & Scientific Research
A Multidisciplinary & Interdisciplinary Journal

Vol. 1, No. 2, September, 2015

Knocking Off Cyberwash: Through the Prism of End-Users

Jejelowo, F.O.
Software Test Analyst/IT Security Consultant
K-LAGAN Technology & Consulting
Barcelona, Spain.
francis.jejelowo@bcs.org.uk

Ademola, E.O.
Professor & CMI Subject Matter Expert,
Trademark Owner of Power-Age (Management Consulting),
Orpington, United Kingdom.
ademolaeo@p-acc.co.uk

ABSTRACT

The Internet became an integral part of human endeavor in the latter part of the last century and did continue into the 21st century thereby leading us to where we are presently. The dependency of human activities on modern technology as it concerns the cyberspace is so huge that it is almost unquantifiable. The relationship between human dependencies on the plethora of modern computer technologies is unarguably symbiotic. Nevertheless, our reliance on computer technology comes with huge challenges, and for the purpose of this paper, the focus is on the *Super Highway* with its greatest challenge of all being "Security"; which this paper seeks to discuss with a view to shedding light on some critical areas of the subject matter, advance ancillary issues and proffering some practical solutions where necessary.

Keywords: Security, Information Assurance, BYOD, Cyber, Cyberwash, Hackers, Hacktivist

.

Aims Research Journal Reference Format:
Jejelowo, F.O. & Ademola, E.O. (2015): Knocking Off Cyberwash: Through the Prism of End-Users
Advances in Multidisciplinary (AIMS) Research Journal. Vol 1, No. 2 Pp 111-114

1. INTRODUCTION

Information assurance (IA) is what information security people do to try and manage risks associated with information and data. This covers the people, processes and systems that might access, store, process, and transmit it. It should be holistic, and focus on more than just technical security controls, taking on board strategic and organizational issues too. IA should consider governance and compliance issues alongside the risks, paying due regard to legal, regulatory and contractual compliance. However, the National Security Telecommunications and Information Systems Security Committee (NST1SSC) define Information Assurance (IA) as Information Operations (IO) that protect and defend information and information systems ensuring their *availability, integrity, authentication, confidentiality, and non-repudiation*. This includes providing for restoration of information systems by incorporating protection, detection and reaction capabilities. [R1]

It is not simply an IT or technical discipline where techies can work in isolation from the real world; often it requires a delicate balance when people and cultural conflict are possible, e.g. with BYOD – Bring Your Own Device.

1.1 Working Definition

"Cyberwash" is the authors' academic derivative to calm information security experts of the fear of daily attack impose on the end users and advocacy for a strengths-focused common approach into absorbing the problem enacted within the viewpoint.

2. ASSESSING INFORMATION SECURITY FROM MULTIPLE ANGLES

When it comes to Information Security, you need to take a wide view of the subject, considering that social media is a rising cultural tide. One would need to take a v-shaped approach as to how the issues surrounding Information Security is viewed if any meaningful solution is to be proffered regarding its exponential increase of security challenges, which are not unconnected with the high increase of sophisticated digital and technical devices that have the capacity to send/share, store and retrieve data through the aid of computer networks.

Other balances must be struck when considering aspects of privacy and transparency, weighing obligations against benefits and risks. A good IA professional tries to rarely say no, preferring to understand what the business is trying to achieve and then working collaboratively with it to arrive at a suitable method of getting the desired result. Those working in IA must continue to stay on top of standards and good practice, advances in technologies and emerging issues that may impact particular approaches and change risk profiles (e.g. online communications and cloud computing being targeted by foreign governments).

Most of all, they must engage positively with their business. Working in this space is challenging, with everything continually developing, and rewarding, especially when playing a part in defending your organization, client or country.

2.1 Holistic Security (HS)

For the IT department, protecting personal data is an on-going concern requiring constant review. The technology provided by employers has changed dramatically over the last decade so that there are more opportunities for data leakage, for instance by way of portable devices. Employers are faced with multifaceted risks, which are broken down into the following categories:

- Cyber criminals making money through fraud or the sale of valuable data,
- Industrial competitors trying to steal secrets,
- Foreign intelligence services, but even with this framework in place, staff-related security incidents still occur which leads us to ask whether the users are taking security seriously.

However, threat of financial penalties with the immeasurable consequences of loss of reputation tends to promote the need for a holistic approach. Only recently it was reported that the personal details of about six million people have been inadvertently exposed by a bug in Facebook's data archive, not too long ago over in South Korea, a cyber alert was issued after an apparent hacking attack on government websites, including the presidential office [R2]. The natural question then to ask is: ***Who masterminds these threats?*** GCHQ (Government Communications Headquarters – the security and intelligence organization tasked by the British Government to protect the nation from threats) [R3] seem to have an answer in what it terms – ***Ten Steps to Cyber Security*** as:

- Hackers (malicious individuals who illegally breaks into computer systems to damage or steal information) in it for the laughs [R4]
- Hacktivists (those who use computers and any other IT systems and networks to debate and sustain a political issue, promote free speech, and support human rights.) with ideological motives [R5]
- Employees or those with legitimate access, either by accident or deliberate misuse.

However, the Department for Business Innovation and Skills reported that for the year to April 2013 the statistics for the number of 'other incidents caused by staff' was actually fractionally higher than that of cyber attackers, at 72 per cent [R6]. This then leads us to the next part of this paper where we are going to discuss how to critically look into cyber-related issues from a non-technical viewpoint.

3. HANDLING CYBER ISSUES USING A NON-TECHNICAL APPROACH: ANALYSIS

It is always a good thing to know that the solution to a problem is multidimensional. That being said, this can only be made possible when a thorough analysis of such problem is conducted, which is what this paper is tend to do in this section. Now let us use the report put together by the Department of Business Innovation and Skills referred to above as a case study: It was gathered that the incidents found over a specific period of time were broken down into subcategories:

A dedicated security professional did say that this is challenging as a wealth of information from diverse sources has to be continuously collated to stay on top of things. There is no single, comprehensive source of knowledge. Instead we inform ourselves by reading, attending conferences and taking advice from experts and our peers.

Following this process we review, what we have learnt and carry out a risk analysis to see how the threats could actually affect us. Once we have carried out a risk analysis, we get together with management and create a hybrid plan of written policies coupled with actions restricting employee behaviour. There are hard choices to be made about whether to prohibit, monitor or allow on trust and rely on the users' cooperation and understanding.

But even with this framework in place, staff-related security incidents still occur which leads us to ask whether the users are taking security seriously. For the IT department it is all too easy to blame the staff for not following instructions whereas in reality, staff-related incidents are often the people and processes affecting the information security behaviour of employees and created a model that serves as a tool for predicting what factors have the ability to potentially impact upon employees[R6].

There will be a 'spectrum of commitment' in most organizations where users will display different behaviours along a scale from total rejection of advice at one end to total acceptance and adherence at the other. Most employees fit somewhere in the middle. The researchers assert that personality affects intention, in that it will act as a filter through which various other influences are passed in order to inform and affect an individual's ultimate security behaviour.

The ability to carry out that intention is then affected by the security safeguards put in place by the organization, such as training, monitoring, disciplinary procedures and proactive security role models. Cormac Herley of Microsoft Research looks at the issue of IT security behaviours from the user's perspective, tackling it from a cost versus benefit perspective [R6]. He suggests that the majority of the advice given is good. However, for the user this type of advice comes at a cost, which is weighed up against the perceived benefits.

He argues that users go through a subtle thought process when deciding whether or not to follow good practice, carrying out a cost/benefit calculation, where the cost is the time and effort involved in following the guideline, and the benefit is subsequently avoiding the harm an attack might bring. So it comes down to direct and indirect costs.

4. CONCLUSION

Security guidelines do help to reduce exposure to the direct costs of an attack, but at the same time the indirect costs, though hard to measure, are increased in terms of time and effort spent implementing the guidelines. So users ignore new advice because they are overwhelmed and the cumulative effort required is a burden. The benefit is perceived to be debatable, combined with the fact that there is a lack of data on the frequency and severity of attacks.

Therefore to the user it appears to be mere speculation that following security advice will reduce the risk of attack. What this means is that we need more detailed research into the success rates of various types of attack to help us to tailor our guidance and avoid 'worst-case risk analysis', allowing us to offer usable advice on the most common exploits such as phishing.

We must prioritise our advice, avoiding cyberwash, otherwise users will have to select which advice they follow and which they ignore and finally we must realize that when we exaggerate all the risks, many users will simply ignore us. In reality, it is practically impossible to attain **100% Security** in any given situation due to the complex nature of the subject matter. However, a lot can be done to achieve a realistic percentage of security if we all acknowledge the fact that the issue of security is a "collective" issue and one that should not be seen as the sole responsibility of a department of an organization or that of IT professionals alone. In other words, all stakeholders (IT professionals, clients, end-users, service providers and government) **must** be involved and to be seen as playing complementary roles in the quest for achieving near-maximum security.

REFERENCE

1. W. Victor Maconachy, Corey D. Schou, Daniel Ragsdale and Don Welch. **A Model for Information Assurance: An Integrated Approach**. Proceedings of the 2001 IEEE Workshop on Information Assurance and Security United States Military Academ, West Point, NY, 5-6 June, 2001. Retrieved from: http://it210web.groups.et.byu.net/lectures/MSRW%20Paper.pdf
   Last accessed date: 7th August 2015
2. **Holistic Security** www.bcs.org/security Last accessed date: 20th July 2015
3. GCHQ **http://www.gchq.gov.uk/who_we_are/Pages/index.aspx.** Last accessed date: 23rd June 2015
4. http://www.computerhope.com/jargon/h/hacker.htm . Last accessed date: 20th June 2015
5. **Hacktivism: Means and Motiviations…What Else?** http://resources.infosecinstitute.com/hacktivism-means-and-motivations-what-else/ Published in General Security, October 2013
6. **Avoiding Cyberwash** ITNOW September 2013 Pages 28-29

Research Materials

7. GOV.UKhttps://www.gov.uk/government/publications/10-steps-to-cyber-security-advice-sheets
   Last accessed date: June 18th 2015
8. OWASP.ORGhttps://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
   Last accessed date: June 18th 2015
9. GCHQ http://www.gchq.gov.uk/press_and_media/news_and_features/Pages/Relaunch-10-Steps-to-Cyber-Security.aspx. Last accessed date: June 18th 2015
10. Andy Taylor, David Alexander, Amanda Finch, David, David Sutton**, Information Security Management Principles, 2nd Edition, 2013**
11. **Common Body of Knowledge Review: Access Control Domain Version: 5:10** http://opensecuritytraining.info/CISSP-8-AC_files/8-Access_Control.pdf
12. Shon Harris, **CISSP All-in-one Exam Guide**, 6th Edition, 2013