Analysis of Human Factors in Cyber Security: A Case Study

ABSTRACT Purpose: This paper critically analyses human factors or behaviours as the major threats to cyber security. Focus is placed on the usual roles played by both the attackers and defenders (the targets of the attackers) in pervasive cyber threats and the potential impacts of such actions on critical security infrastructures.

Design/Methodology/Approach: To enable an effective and practical analysis, the Anonymous attack against HBGary Federal (A security firm in the United State of America) was taken as a case study to reveal the huge damaging impacts of human errors and attitudes against the security of organizations and individuals.

Findings: The findings revealed that the powerful security firm was compromised and overtaken through simple SQL injection techniques and a very crafty social engineering attack which succeeded because of sheer personnel negligence and unwitting utterances. The damage caused by the attack was enormous and it includes the exposure of very sensitive and personal data, complete shutdown of the website, loss of backup data and personnel character deformations. The research also found that damaging human factors results from ignorance or illiteracy to basic security practices, carelessness and sometimes sabotage by disgruntled employees from within and these vulnerabilities have become prime target for exploitation by attackers through social engineering attacks. Social engineering was also discovered to be the leading attack technique adopted by attackers within the cyber space in recent years.

Practical Implications: The paper concludes by advocating assiduous training and cyber security awareness programmes for workforces and the implementations and maintenance of basic security culture and policies as a panacea for social engineering cyber attacks against individuals and organizations.

Originality: Lots of work has been done and many still ongoing in the field of social engineering attacks and human factors, but this study is the first to adopt an approach of a practical case study to critically analyze the effects of human factors on cyber security.

Keywords: *The Anonymous; HBGary Federal; Uniform Resource Location (URL); Content Management System (CMS); SQL Injection; Cross-site Scripting (XXS); Social Engineering; Cyber Security; Information Security*

Paper Type: *Research Paper*

1 Introduction

Humans have been found to be truly the weakest link of security (Mitnick, Simon, & L., 2011) and (GBC-DELL Survey, 2015). The psychology of human workforce is being viewed as a critical factor that poses serious cyber-attacks risks to all users (Ranjeev & Lawless, 2015). Human cyber security behaviours has created serious vulnerabilities which attackers exploits using social engineering attack techniques and findings revealed that human factors are responsible for 95% of all security incidences (IBM, 2015). Human threats to critical infrastructures and services come mostly from careless work behaviours and ignorance of basic cyber security practices which include irregular software patching to get rid of bugs, installations of malicious software, careless communication of sensitive information and connection to insecure internet networks or Wi-Fi (Aziz, 2013) and (James, 2015). They also include poor attitudes to web applications usage and database management which opens door to cross-site scripting (XXS) and SQL Injection vulnerabilities (Stuttard & Marcus, 2011). Attackers these days find it interestingly easier to begin their attacks by the exploitation of human ignorance, weakness and selfish interests to gain an open entrance for a mega attack. People are now inadvertently deceived to either initiate or even carry out the attacks by themselves without the attacker necessarily introducing an external event or involving very expensive technical exploit kits. Human factor is an insider threat against security either through disgruntled employees seeking to cause pains or through social engineering which appeals to personnel's instincts and attackers would rather take advantage of these vulnerabilities, where available, than engaging other exploits against technical security devices (James, 2015), (Warwick, 2016) and (CeBIT Australia, 2017).

Research has shown that it is not good enough to have all the state-of-the-art security software and hardware properly installed and running in an organization if the human factor to cyber security is neglected (Nate L. , 2016), and (James, 2015). Firewalls, Intrusion Detection Systems, Antimalware and many authentication mechanisms such as time-based tokens or biometric smart devices, are usually installed to protect against external threats but cannot protect against threats from within, caused by ignorant and careless personnel (Mitnick, Simon, & L., 2011) or by disgruntled employees aiding external attacker (Blythe, 2013). Cyber attackers would rather now want to exploit the vulnerable human factors through simple tricks than to spend much time and resources trying to gain access by breaking through the different strong technical security systems. This paper seeks to practically analyze the impacts of human factors to critical security infrastructures. The attack of the Anonymous Hacktivist group against HBGary Federal, a US based security firm, was taken as a case study to analyze the different phases of cyber attacks against human cyber security behaviours. The different phases include the analysis of defender(s) vulnerabilities (target of attack – the human factors), the analysis of the attackers' tricks and techniques, and finally, the analysis of the resulting damages. The paper concludes with suggestive techniques for preventing against such exploitations.

2 Social Engineering

Social engineering is a non-technical method of cyber-attacks which absolutely depends on human psychology and mostly involves deceiving people into breaching standard security practices (Nate, 2016). Researches have shown that social engineering attacks are the top most threats against information security (Warwick, 2016) and (Nate, 2016). The whole technique of social engineering attacks is completely anchored on the principle and art of deception, making people do things that they would ordinarily not want to do for a complete stranger (Mitnick et al, 2011). Thus, victims of this attack techniques are usually persuaded to willingly open wide their security door ways to unknown persons (Ranjeev & Lawless, 2015) or are tricked to do things like giving out sensitive information or documents, disabling critical security systems, transferring money to unknown persons' accounts and many other devastating things (Warwick, 2016). Sometimes they are tricked to believe that the order they are obeying is coming from a superior, colleague, or partner sitting somewhere (Mitnick, Simon, & L., 2011). Often times, what they are persuaded to do are highly regrettable, causing irreversible damages.

Common approaches or attack vectors adopted in social engineering attacks include engaging people through fake emails, social media, voice calls, mobile apps, or through direct physical contact with the defendant (target of the attacker). Social engineering attacks, or attacks against human psychology and instincts, may come in the forms of phishing, malware attacks, pretexting, baiting, quid pro quo and tailgating (David, 2015). Phishing scams and malware infections have be found to be the most adopted forms of social engineering attacks (GBC-DELL Survey, 2015) as indicated in Figure 1. Anyone that falls victim of social engineering attack would normally become the enabler of the bigger attack or might even unknowingly be used to directly complete the full-scale attack.

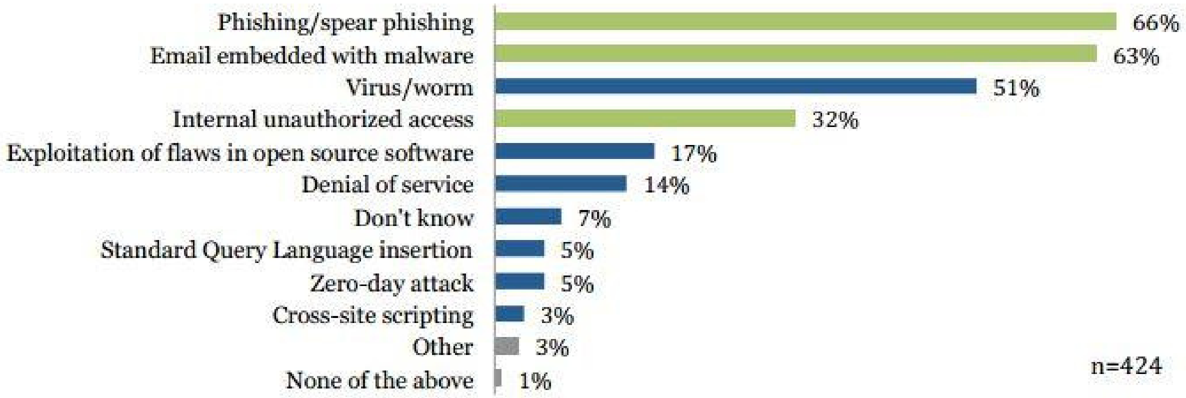

Figure 1: Significant Cyber Threats (GBC-DELL Survey, 2015)

This study takes a deep delve into some practical applications of social engineering attacks and its requisite consequences and prevention. The attack of the Anonymous Hacking group against HBGary Federal security firm was adopted as a case study for a critical analysis of this attack technique. The study begins by critically looking into the different services offered by HBGary and where they failed. A brief about the Anonymous group was also discussed; the different attack techniques deployed, the resulting damage, ways of preventing similar attacks on businesses, and the lessons learned form the core of this study.

3 The Defender – Hbgary Federal

HBGary was a well-known technology security company with offices in Washington D. C.,

California, Sacramento, and Bethesda, Maryland. The Security Firm was founded by Greg Hoglund in the year 2003. The company entered into a Security Innovation Alliance with McAfee in the year 2008. The Establishment was an affiliation between HBGary Federal and HBGary Inc, both being very distinct entities. HBGary Federal had one mega web server which could be accessed through a Web link, *www.hbgaryfederal.com*, and they also had one major Support Linux Machine which could be accessed through the link, *support.hbgary.com*. The Linux Machine contained most of the employees shell accounts, which they could access using SSH. Greg Hoglund also operated another website called Rootkit.com which was hosted by another Linux machine. All the email

services of HBGary Federal were being managed by Google Apps. The National Security Agency (NSA) and Interpol had maintained a frequent contact with HBGary companies and HBGary also had been working with McAfee which is a well known security firm too (Peter, 2011).

HBGary Federal, being an information security firm, specializes in design and distributions through sales of the state-of-the- art tools for computer forensics and malware analysis to the United State government and other private Institutions (Peter, 2011) and (Krebs, 2011). Their services also included technical consultancy and supports. The support covers areas such as the implementation and deployment of intrusion detection systems, designing secure networks, performing vulnerability assessment and penetration testing of systems and software. The United State Government and some Strong Private Organizations were some of the patronisers and customers of the services of HBGary Federal.

4 The Attacker – Anonymous

The Anonymous is a group of hacktivists which comprises of people from different backgrounds, diverse professional experiences and different age groups. This involves professional office employees, software developers, IT technicians, and even students. The membership of the group are found scattered in different countries of the world, a few amongst them includes the United

State, Germany, The United Kingdom, Netherlands, Italy, and Australia. The hacktivist group mostly adopt cyber attack as their main campaign medium to show their displeasures and grievances against any government policies or any Organization that might have crossed their ways. The group was allegedly founded in the year 2003.

A few amongst many other exploits perpetrated by the Hacktivist Group includes the bringing down of PayPalblog.com, MasterCard.com and Visa.com (Nate & Technica, 2011). The attacks against these Companies were done to punish the financial companies for their involvement in shutting down WikiLeaks from the internet. Anonymous attacked these websites using Distributed Denial of Service (DDoS) attacks through a modified version of the Low Orbit Ion Cannon (LOIC) load-testing tool.

5 Human Factors Vulnerabilities Analysis

HBGary was operating a content driven website whose data was stored in an SQL database. As it is with every thriving business, there was always a constant need for updating the contents of the website by correcting, adding or removing some information from the database. To make the administration of the website easier, HBGary Federal deployed a Content Management System (CMS) in the organization. Although this approach was a good idea, but best practice would have been for them to implement an off-the-shelf Content Management System which would have enabled them the ability to directly monitor and control the system, but they rather chose a custom CMS from a third-party developer. Third party's applications do not always have good reputations as they mostly have issues with malware and wrong coding (Rahul, Venkiteswaran, Anoop, & Soumya, 2014), so the CMS deployed by HBGary had serious coding flaws which made it highly vulnerable to cyber attacks. Although the CMS had bugs, HBGary was negligent and careless about the CMS. They could have exercised their own expertise as security experts in finding and fixing (debugging) the bugs and also setting up and configuring bug tracking devices to track security vulnerabilities of the software, but they failed to do any of this. HBGary was completely blind to this dangerous flaw, allowing the CMS to become highly vulnerable to SQL injection attacks.

The Security Firm, HBGary Federal, was also guilty of poor password management. The senior executives of the Firm, CEO Aaron Barr and COO Ted Vera, became too busy about their work that they forgot and neglected simple and standard information security practices especially in the areas of password policies and management. They became an extreme bad example to be emulated in this regard. Both top Officers had extremely weak passwords with each comprising of only six lower case letters and two numbers. As though that was not bad enough, they also maintained the same passwords across platforms and applications. That is, the same password was used to login into their twitter accounts, email accounts, LinkedIn, and SSH. This practice subjected them to a security single point of failure (failure at one point implies failure at all points). The most disturbing part of it was that Aaron had the administrative right over the Google App that hosted the entire company's emails and while Ted had a user privilege in the Linux SSH account. Password misuse and negligence alone had exposed the Company to serious security threats.

In managing the SSH access to the Firms Server, the authority also carelessly ignored the principles and policies governing safe SSH connections. It did not come into their minds to remember that password authentication was not the best security verification practice for any SSH connection, so they continued to use only passwords to gain access via SSH to the Support Linux Machine. They could have included the hard-to-crack cryptographic encryption methods in the system which would provide each user with a secret key which must be kept private and with a public key that is associated with the user account. If these were put in place, the SSH would have then made use of both keys to authenticate the different users. The Firm adopted MD5 for their password encryption in a very weak way. Another serious security loophole entertained by HBGary Federal was inadequate software patching. Little or no attention was given to regularly patching the Linux Support Machine. This also exposed the Machine's Operating System and its system libraries to privilege escalation exploitation attack vulnerabilities.

Finally, there was serious lack of proper information dissemination within and outside the Company. They were very careless at releasing very sensitive information without minding who is listening. This attitude exposed the Corporation to the subtle danger of social engineering attacks. The Anonymous shows up mostly through cyber attacks, so they have been associated with majority of cybercrime in the world. Because of their activities, this Group became a prime suspect to the United State Government and this has set them on the list of the FBI for continuous investigation to uncover the identities of its members (Nate & Technica, 2011). The CEO, Aaron Barr, was too outright and straight, without caution, when he publicly announced the Firm's collaboration with the FBI (Federal Bureau of Investigation) against the Anonymous group. He revealed that the Firm had gotten some essential information about the identities and activities of some cardinal members of the Anonymous group, expressing his readiness to sell this information out to the FBI for further actions against the group. The method he claimed to have used in getting these essential details was emails monitoring, and using of fake names for Facebook and IRC chat. His action presented him as having a boast on the strength of the Firm and their victory over the Anonymous group (Nate & Technica, 2011). This pronouncement was regrettably a dangerous move that invited the wrath of the hacktivist group, Anonymous, against HBGary Federal. Without hesitation, the Anonymous reacted immediately against Aaron's moves by attacking HBGary Federal between the 5th and 6th of February 2011. The attack lasted for a period of 24 hours only.

6. Analysis of Attackers' Techniques And Tricks

Anonymous started by exploiting the vulnerability found in the Content Management System (CMS). They injected some SQL queries into the Firm's web server database. The coding of CMS are meant to enable it identify what details it should allow to be retrieved from a database system based on the receipt of a particular query or URL (Uniform Resource Location). The CMS is required to match the received query against the records in the database, render the collected content which may include an HTML, and then countless web pages can be created within seconds to display the required results. A typical CMS would usually have a web 'front-end' which allows the editing of database records through the web by the respective users. The SQL query injected by the Anonymous made use of the URL, **http://www.hbgaryfederal.com/pages.php?pageNav=2&page=27**. Two parameters included in the query to manipulate the CMS are pageNav=2 and page=27. Given that the CMS had bugs already in its code, it became easily tricked to misinterpret the query with these parameters, thus providing the hackers with open access to the database of the web server that hosted the Firm's very sensitive data. They completely took over the database from the CMS. Some details retrieved from the database include usernames, email addresses, and password hashes of privileged users who had the administrative right to make any required changes to the CMS. The vita data found on this server provided the attackers with more information that aided their invasion further. One good property of the CMS was its ability to store only the hashed password of the users in the database which could be very difficult to break into plain text. Fortunately for the attackers, the hash was only a single one-way hashing that was done using MD5 hashing function without applying salting and iterative hashing methods. Taking advantage of the weak hashing procedure, the attackers deployed rainbow table cracking technique to crack the downloaded hashed passwords. Iterative hashing involve the process of having the output of a hash function re-hashed again repeatedly for several times (Sjoerd, 2016) and (Dunkelman & Eli, 2006), while salting technique involve adding a small amount of random data to the password before it is hashed (Sjoerd, 2016) and (Patel, Patel, & Virparia, 2013). If these hashing techniques were adopted, it would have become either very difficult or nearly impossible for the passwords to be cracked by the attackers. It suffices to say hbgaryfederal.com would have survived the rainbow password cracking attacks despite the loophole found with the MD5 hashing functions if they probably had adopted the best password protection policy (Daniel, 2015) and (SANS, 2014).

Rainbow table attacks commonly succeed against two kinds of password patterns; this include password of eight character length which compromises a mixture of lower case letters and numbers only, and a those of one to twelve character length which are made up of upper case letters only and anything outside these lengths, it becomes extremely difficult for the rainbow tables to generate (Avi, 2016) and (Coding Horror, 2007). Although CEO Aaron Barr and COO Ted Vera were expected to know better, given that they owned administrative rights to different systems, they both were still very careless to use password combinations of only six lower case letters and two numbers. Another huge mistake made by these executives was the reuse of same password on different platforms and applications including even the Support Linux Machine, *support.hbgary.com.* The attackers took advantage of this weakness and were able to easily attack the Linux Machine using Ted Vera's password. Unfortunately, the

Linux Machine had some software vulnerabilities due to inadequate patching, so the attackers deployed privilege escalation exploits to gain root privilege and had total control over the machine from where they extracted gigabytes of backups and research data.

The password for Aaron Barr was used by the attackers to gain administrative access into the Google App that controls the entire Company's emails. Greg Hoglund, the founder and owner of rootkit.com, had his e-mail account also listed there, so the attackers accessed his email and were able to retrieve two additional passwords from there which were '88j4bb3rw0cky88' and '88Scr3am3r88' which could give them the root access to the server hosting rootkit.com, but they also found out that Jussi Jaakonaho (Chief Security Specialist) of Nokia had a root access to the machine too.

Despite the details retrieved, it was still impossible for them to break into Greg's machine by direct SSH using root account (username & password), they would need to first login with a non-root privilege user account. The root account details could not be used to access the server from outside of the firewall and so they sought for ways to retrieve Greg's common user account details (username and password) (Keir, 2011). They resorted to social engineering attack using email (Peter, 2011) against Jussi Jaakonaho from whom they were able to get all the details they needed to complete their task. To implement the social engineering attack, the attackers disguised as Greg Hoglund by using

his email account to send mails to Jussi Jaakonaho.The email conversations between the attackers and Jussi are as follows (Peter, 2011):

6.1 The Impact of Human Factor on Critical Infrastructure

The HBGary website was completely compromised, over sixty thousand(60,000) Company emails were downloaded and exposed on The Pirate Bay site (Chester, 2011). The Company's backup files were completely deleted by the Anonymous. The Group also retrieved and publicly displayed the documents HBGary Federal boasted about earlier to sell to FBI for everyone to see. They also retrieved and exposed users' database from Rootkit.com and all the email addresses and passwords hashes for everyone who had ever registered on the website. Aaron Barr's private and confidential credentials which include his private mails, home address, social security number and cell phone number were all exposed to the public. The greatest damage was on the Integrity, Reliability, Confidentiality and finally the Availability of the Company. The mistakes were completely irreversible resulting to a total shutdown of the security Firm, HBGary Federal, putting them out of business.

7. How To Prevent Similar Attacks On Businesses

Staff trainings on standard security principles and policies must be taken very seriously in every Organization in order to combat social engineering attacks (GBC-DELL Survey, 2015). This will be an essential tireless and continuous cybersecurity literacy and awareness training for the workforce. It is worth spending resources on keeping the security and risks management knowledge of workers updated all the time as this can reduce an organization's cyber security breaches by 70% (Pittsburgh, 2015). Proper policy must be put in place with the right password hashing techniques especially the use of iterative hashing and salting. A regular vulnerability testing of website must be carried out to look for security holes in order to cover them up. Public and private key encryptions and authentication techniques should be deployed for protecting the server when it comes to authentications. Systems and software patching should be done on regular basis. Vulnerability assessment must be done on all the information infrastructures deployed in the network. The practice of password reuse on different platforms should never be encouraged. Social engineering is a very subtle attack, thus personnel should always verify any requested task before agreeing to release very important details.

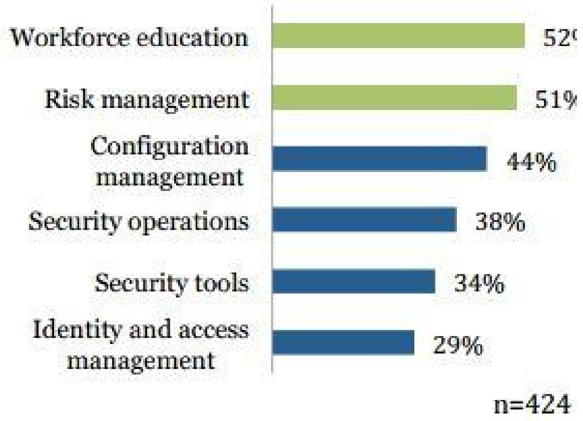

Figure 3: Cyber Defense Elements in Need of Significant Improvement (GBC-DELL Survey, 2015)

8. Conclusion The case study analysed in this paper suggest that attackers will not usually attack from areas that are considered to be of great security strength, but would rather focus their attention on the very weak and neglected points of security, especially the human factor. Human factor was the greatest weakness that brought down HBGary Federal. They were too busy rendering security services to their clients that they failed to maintain positive attitudes in securing their own IT their massive negligence and vulnerable infrastructures. The little things they neglected became their biggest problems; no one would have expected such from an established security Firm like HBGary. The fall of HBGary is a clear indication that the bad guys are always a step ahead in their calculations, and they see tiny security lapses that are usually oblivious to security experts**.** Hence, this is a huge lesson to be learned by every individual, corporation and security professional, to stay equipped and wel Danish, informed about standard security practices, maintaining positive security behaviour always. It is therefore very imperative that great security culture demands that nothing, however simple or irrelevant in appearance, should be treated casually when it pertains to security. Finally, it is expedient that keeping a healthy cybersecurity work behaviour, cyber hygiene, and organizational planning is as core to information security as firewalls and anti-malware.