Hacking

1. **Introduction**

The rise in the use of information and telecommunication technologies (ICT) in our daily lives has led to an increased reliance on virtual networks in conducting ordinary day-to-day tasks as the use of web-based technologies becomes the norm. However, the use of web-based technologies also exposes individuals to risk of attack from cyber criminals that have varied motives in carrying out attacks. The prevalence of ICT has led to the mainstreaming of the term hacking, as cyber security experts and ordinary people worry about the security of personal information as well as the system itself from hacker attacks. Thomas (2002) argues that the term hacker has a double meaning although the popular perception of the word tends to be one-dimensional. Hackers are popularly conceived as persons who are engaged in technological mischief or even criminality by using their knowledge and ability to exploit ICT systems for their own, mostly illegal interests. However, originally, in the tech-savvy community, the term was of the highest approbation, referring to individuals with the ability and imagination to generate clever technical solution through non-conventional means (Coleman, 2010). Due to the notoriety of the hacking incidents exposed by the media, the former meaning of hackers has taken root and there tends to be little understanding of the subtle differences between the different categories of hackers. It is imperative to note that both definitions of a hacker acknowledge that the hacker has superior ability and can manipulate technology to his will giving, an ability that can either be revered or a source of fear. Consequently, there has been a concerted effort by government agencies to criminalize hacking and institute aggressive measures to guard against hacking as well as track and nab hackers (Thaw, 2013).

Gold (2014) analyses the psychology of hackers and claims that hackers can be categorized as ‘white hats’, ‘black hats’ or ‘grey hats’ depending on the motivation in engaging in hacking. White hats are mainly interested in seeking out flaws in the IT infrastructure and systems with the aim of rectifying these flaws for the public good and their work usually collaborated with that of security agencies wittingly or unwittingly. Black hats on the other hand tend to be individuals with psychological disorders like obsessive compulsive disorder, are addicted to the ‘thrill’ of hacking and often use their hacking ability for nefarious purposes. Lastly, the grey hacker or ethical hacker is emerging, and these are individuals that help to check on the resilience of organizations’ defenses by assessing whether the defense can be cracked. Hampson (2012) notes that a new form of protest, which he calls hactivism, has emerged recently as people use the internet to express their displeasure with what may be happening. An appropriate example of this new form of protest was seen after the corporate backlash against WikiLeaks for publishing classified US documents. After WikiLeaks suffering from denial of service (DOS) attacks that made the website unstable as well as expulsion by hosting providers, an online group of hackers emerged who began to attack the corporate entities deemed to oppose WikiLeaks with DOS attacks. Although hacking may be detrimental to the security and privacy of individuals, western democracies have enshrined the right to protest, and there may be need to protect hactivism, which is the non-violent use of illegal or legally ambiguous tools for political ends.

1. **The Gucci Hack Attack**
	* **The Incident**

On 12th November 2010, the Gucci network in America was disrupted massively, leading to loss of access to the network for a period of approximately 24 hours. The network disruption attack led to not only denial of service but also the loss of valuable company data, including documents and emails, both personal and corporate (Liebowitz, 2011). For the 24 hours that the network was down, the company lost all access to any of its documents, and some documents and emails were permanently lost even after the network was restored to full functionality. This is because during the network disruption attack, the hacker deleted the documents and emails leading to the permanent loss of data that was not backed up. Even after the network was restored to functionality by Gucci network administrators, the after effects of the attack lingered on for a considerable amount of time as the administrators tried to repair the damage caused by the hack. The network disruption attack led to Gucci losing a substantial amount of business over the day as customers could not access any of its online stores in the US. In addition, the company lost valuable documents that had taken considerable working hours to prepare.

* **Background**

Sam Chihlung Yin was an IT expert working for the luxury goods dealer, Gucci, in America as a network administrator for the company’s in-house information system. Yin was accused of abusing employee privileges by buying goods from the retailer in bulk and then selling them off to the Asian grey market at a profit. The retailer subsequently fired him in May 2014 for the misdemeanor, which was unrelated to his core competency (Shell, 2012). However, before he left the company, Yin used his technical knowledge to create a fake virtual private network (VPN) network token, which he took and then later called Gucci IT department and tricked them into activating the token as if he was a new employee. With his active credentials, Yin used his administrator-level passwords to have a virtually unfettered access to Gucci’s network although he no longer worked there. Between the time of his sacking and November of 2010, Yin kept tabs on what was happening at Gucci and it is alleged that he illegally accessed sensitive company data and made copies of the data. On 12th November 2010, he systematically shut down storage areas, wiped corporate mailboxes and other data and deleted various virtual servers that were running Gucci’s network, crippling the network for nearly 24 hours before it was restored by administrators.

* **Consequences Of TheGucci Network Attack**

The immediate effect of the hack was a collapse of the Gucci network, making it impossible for the company shop managers to keep in touch with headquarters as well as for customers to access the company’s online shopping facility. The company lost valuable working hours as network administrators struggled frantically to bring the network online, and shop activities were paralyzed, as the shop managers could not access the inventories from the network’s storage. The company also lost corporate and personal emails as well as other data that was not backed up. It is estimated that the hack, which caused network disruption for a full working day caused damage and lost productivity estimated at $200,000 (Leyden, 2011). In addition, the loss of virtual services hurt the image of the company, as frustrated customers could not access the company’s store.

* **Analysis Of The Hack**

The system hack was not achieved through attacking the network through its weak points but through playing on the human element of the system. By deceit, Yin managed to obtain access to the system after convincing the system administrators to activate his access, opened in the name of a fictitious employee. Therefore, although the network was hacked, it is not certain that the network itself has vulnerabilities, which can be directly attacked externally by a hacker. The hack of Gucci was motivated by revenge and malice on the part of Yin, following his dismissal from work. Although he had near unfettered access to the retailer’s network for a number of months, there is no conclusive evidence that Yin used the data he accessed during that period for any purpose. He seemed to have just enjoyed accessing his former employer’s network before deciding to cripple it to get back at his employer. Yin’s actions cannot be attributed to any ideological reasons or personal ideals. He might be considered as a person who is psychologically maladjusted and cannot accept adverse situations and adjust accordingly. Although he has a vendetta against Gucci, there is no suggestion that he was wrongfully terminated, and his actions shows him as an emotionally unbalanced person, who fits perfectly into the ‘black hat’ characterization.

The attack on Gucci occurred because the human aspect of the system has weaknesses that can be exploited, bypassing the security firewall and gaining access fraudlently. The authentication protocol seems to be so weak that administrators can activate the access for a fictitious employee without cross-checking the credentials of the employee. In addition, there seems to be a laxity in deactivating the passwords of employees who have left the organization, making the system vulnerable to internal attack. Yin was able to use his administrator passwords even after being sacked, which is a serious oversight by the company IT department.

1. **Preventive Measures**

Gucci has an internal employee benefit program that allows employees to obtain goods at a subsidized price. However, the system is open to abuse, forcing the company to take precipitous action against employees, which is likely to cause resentment and motivation for revenge, implying that the company’s reward systems should be structured such that it reduces the chances of abuse. The company should also explore alternatives to employee discipline rather than resorting to summary dismissals, which are likely to motivate employees into contemplating revenge to spite the company.

1. **Mitigation Measures**

The authentication protocols in the company should be strengthened to ensure that only genuine employees are activated in the system. There should be safeguards to ensure that before any new employee is given access into the network, the IT department liaises with HR to verify the credentials provided by new employees. The company should also limit access to the number of people who have administrator level passwords to ensure that any breach in the network can be quickly detected before the problem snowballs. Since there will always be movement of employees into and out of the company, it is important that up-to-date data on current employees is maintained at all times. The system should be automated such that whenever an employee is removed from the active employee list, all access to the system by the employee is immediately blocked and any passwords that the employee had are deactivated.

References

Thomas, D. (2002). *Hacker Culture*. Minneapolis: University of Minnesota Press.

Thaw, D. (2013). Criminalizing hacking, not dating: Reconstructing the CFAA intent requirement, 103. *Journal of Criminal Law & Criminology 103*(3), 907-948.

Hampson, N. (2011). Hacktivism: A new breed of protest in a networked world. *Boston College International & Comparative Law Review, 35*(2), 511-542.

Coleman, G. (2010 Sep 21). The anthropology of hackers. *The Atlantic.* Retrieved from http://www.theatlantic.com/technology/archive/2010/09/the-anthropology-of-hackers/63308/

Liebowitz, M. (2011 April 5). Frustrated ex-employee hacks Gucci corporate networks. *NBC News.* Retrieved from http://www.nbcnews.com/id/42435505/ns/technology\_and\_science-security/t/frustrated-ex-employee-hacks-gucci-corporate-networks/

Leyden, J. (2011 April 5). Fired Gucci IT worker accused of tearing up network. *The Register.* Retrieved from http://www.theregister.co.uk/2011/04/05/gucci\_bofh\_revenge\_hack/

Shell, M. (2012 July 18). Fired employee admits to hacking Gucci. *MediaTec Publishing Inc.* retrieved from http://www.workforce.com/articles/fired-employee-admits-to-hacking-gucci