## 4.1.1 The existing risks of social media utility across Kenyan enterprises.

### 4.1.1.1 Cyber loafing

Most staff-related incidents normally involve staff misuse of the Internet or email. Cyber loafing number of firms such as G4S and Child Welfare Society of Kenya (CWSK) have been forced to come up with policies on how employees access social media during office hours. They have also invested in filtering and antivirus tools. Employees are normally doing unproductive activities like chatting, surfing the Internet, downloading videos and music during office hours, activities that are bandwidth-hungry and slow the speed of internet for those using it for business.

* + - 1. Data leakage

Kenya cybersecurity report 2015 by Serianu, many companies in Kenya have allowed their employees to take their devices to work, and hackers are taking advantage of poor security on the gadgets to access sensitive company information. “With the continued adoption of enterprise mobility, a growing percentage of workers are using their personal devices to access corporate resources,” states the report. “When these devices are not secured this introduces a wide range of security threats. “People may be inclined to share information on the Internet that their employer would have preferred to keep private. Individuals may not be divulging trade secrets, but the cumulative effect of small, seemingly innocuous details can enable a business's competitors to gain valuable intelligence about that company’s business situation and future plans. (Serianu, 2016)

* + - 1. Social media squatting

Cyber-squatting is becoming more common each and every day in Kenya. Both celebrities and Government officials alike are being targeted by cyber squatters. Enterprises are also not left behind in this, we got people who masquerade as genuine company accounts on Facebook, Twitter, and LinkedIn. They are mainly known to target large organizations.

Phishing

More than 5,000 Kenyan Facebook users have lost millions of shillings in a social hacking scam that lasted for a year, as revealed by a local cyber security firm, Serianu. The firm revealed that it unmasked a Kenyan who broke into personal accounts of Facebook users in Nairobi, Mombasa, and Eldoret and used the access to solicit funds from thousands of people linked to the breached accounts.

4.1.1.4 Reputation risk

Social media being undoubtedly one of the most powerful forms of online marketing. However, it takes time, focusing to get it right, skill set that needs development over time. As a matter of fact, if you do it the wrong way, social media could end up working against you. A case where RMA motors tweeted to a client to have a cold beer in lieu of service. This was is in a response to a complaint from the high profile client to the effect that his brand new Range Rover was always breaking down. The actual Tweet read, "will be in touch to discuss one-to-one your outburst here & what can be done. For today; have a cold tusker & enjoy the day." Within hours, this Tweet had gone viral with hundreds of Kenyans on Twitter expressing their outrage. This describes a classic example of how social media can go wrong if unskilled or inexperienced people in charge of such channels. ("5 Reasons Kenyan Businesses Should Embrace Social Media", 2016)

### 4.1.1.5 Cyber bullying

Cyber-bullying is defined as publishing materials about a victim severely defaming and humiliating them. It isn’t something that anyone or large corporate would want to be associated with. Ironically in Kenya, many companies and personalities actively take part in it by quickly aligning their digital content to a widely known unrelated trending topic. A case in point is during a wave of the #PoleKwaMwirigi tweets, retweets, Facebook jokes and funny memes on twitter which went viral globally through Kenyans on twitter (KOT).Enterprises that apparently took part in the hashtag included: Airtel Kenya, Cold Stone Kenya, Fast Food Restaurant Kentucky Fried Chicken (KFC) and lastly NTV one of kenya’s leading broadcaster also took part in the conversation according, Chacha,(2016).

* + 1. Mitigations strategy

To effectively control social media use by both employees and enterprises, a well-documented strategy need to be developed, with the input of all the relevant stakeholders. This includes: the business management, the human resource, officials entitled for risk management, and the legal representation. An approach of this perspective by holistically integrating emerging technologies into the business will help to ensure risks are considered, with the view of the broader business objectives. A strategy to address the social media risks, should focus primarily on user behavior, with the development of policies and offering support for training and awareness programs which covers.

* Individual use in the workplace:
* Is it allowed or not
* Is it a nondisclosure of business oriented content
* Is it a discussion of work related topics
* Inappropriate content and conversations
* Individual use out of the workplace
* Nondisclosure of business oriented content
* Ordinary disclaimers for employee identification
* The hazards of posting a lot of personal information
* Business/Enterprise use
* Is it allowed
* Is there a process to gain approval for use
* What is the scope of information allowed to flow
* What are the disallowed activities
* Consider the escalation process for consumer related issues.

Proper training and education are imperative, vulnerabilities of social media usage should be well apprised to every employee. Organizations can also consider. A standard “Social Media Safety 101” class as a good starting point. Consequently, a compact and all-inclusive social networking policies should be put in place, and enforced through continuous monitoring leveraging the intelligence tools such as sentiment analysis, for monitoring real-time posts. In addition a proactive, continuous monitoring is highly essential for success, hence all organizations should take responsibility by knowing the greatest goal beyond these social media sites.Lastly, business departments must subscribe to a solid organizational feedback loop. This is with regards to the common tendency for departments to point the finger to another department. Businesses should consider the fact that whenever a breach occurs it is more than just a public relations issue, or rather, just a normal security, legal IT, human resources or security issue. Every department has a specific role to play which can either make or break an organizations social media policy.