The Journal for Transdisciplinary Research in Southern Africa
ISSN: (Online) 2415-2005, (Print) 1817-4434

Narrative review: Social media use by employees and the risk to institutional and personal information security compliance in South Africa

Authors:
Obrain T. Murire[1]
Stephen Flowerday[2]
Kariena Strydom[1]
Christoffel J.S. Fourie[3]

Affiliations:
[1]Department of People Development and Technology, Faculty of Business Sciences, Walter Sisulu University, East London, South Africa

[2]Department of Information Systems, Faculty of Commerce, Rhodes University, Grahamstown, South Africa

[3]Department of Research Development, Faculty of Science, Engineering and Technology, Walter Sisulu University, East London, South Africa

Corresponding author:
Kariena Strydom,
kstrydom@wsu.ac.za

Dates:
Received: 04 July 2020
Accepted: 14 Nov. 2020
Published: 18 Feb. 2021

How to cite this article:
Murire OT, Flowerday S, Strydom K, Fourie CJS. Narrative review: Social media use by employees and the risk to institutional and personal information security compliance in South Africa. J transdiscipl res S Afr. 2021;17(1), a909. https://doi.org/10.4102/td.v17i1.909

Read online:
Scan this QR code with your smart phone or mobile device to read online.

Social media platforms have become essential to organisations in developing countries as they can offer a business advantage. This comes with security risks and privacy concerns as numerous scientific literatures have testified. Although the majority of employees are using social media privately and at the workplace (using the same device such as a smartphone), some organisations have not effectively established information security awareness programmes to protect their electronic information backbone. It is a fact that professional hackers are prowling constantly to gain access to systems of organisations and sometimes employees make naïve mistakes that can open the door to cyberattacks, which exploit vulnerabilities in the organisation's system. The current Coronavirus Disease 2019 (COVID-19) crisis is a prime example where employees and students are encouraged to work from home. No organisation does have complete control over the security measures each employee has in place for his or her private connection. This study applied a desktop review to identify the cyber risks associated with social media use at the workplace. A scoping literature review gathered the data following a qualitative approach. The theories of reasoned action and deterrence were used as a theoretical foundation for the study. A model is proposed to enhance employee information security compliance when using social media at the workplace and demonstrates how awareness strategies can be employed to improve employee information security compliance. It is recommended that organisations implement methods to minimise social media risks to ensure that the integrity of information is preserved through these awareness programmes to employees.

Keywords: COVID-19 pandemic; cyberattacks; information security awareness; internal control; punitive measures; risk; social media; social media policy.

Introduction

The use of social media is soaring worldwide as employees seek to gain access to their organisation's information through their mobile devices and laptops, especially during the current Coronavirus Disease 2019 (COVID-19) pandemic.[1] With the increased number of social media accessed through these digital devices, there is an amplified number of prospective cyberattacks to organisations, which includes network attacks, the spread of malicious code, as well as ransomware.[1,2] Information security breaches, leading to the disclosure of sensitive information, reputational damage and increased threats from cyberattacks on social networking tools has pointed to the need for information security management in organisations.[2,3] For this reason, organisations should be actively involved in information security awareness programmes as social media risks are ever-increasing.[4,5] According to Frauenstein and Flowerday[6] technology controls alone cannot deal with social media risks; therefore, employees play a vital role in the defence.

South African National Standards (SANS)[7] states that whilst organisations already have management controls, technical controls and operational controls, a very important aspect is lacking, which is the human control of 'a human firewall'. The human firewall, with proper training, will contribute to ensure that social media risks are dealt with and reduced to levels that are acceptable whilst enjoying benefits when using these platforms in question. Furthermore, this may ensure that confidentiality, integrity, availability (CIA) and privacy of information in organisations are preserved.[6] Working from home seems to be gaining ground across the world, which is receiving new interest now because of the COVID-19 pandemic.

This study of South Africa focuses on and examines the cost-saving implications involved in companies if their employees would be able and allowed to work from home and the link

between structural and relational factors married with virtual work. The results indicated that the relationship between structural factors and relational factors with perceived virtual work experience is said to be positive. Professional isolation and job performance was found to be highly negatively correlated. Aloul[4] and Ajzen and Fishbein[5] notice a rise in phishing attacks, for instance, malspam and ransomware attacks as COVID-19 is used by attackers as bait to impersonate brands and mislead employees. This puts personal computers and phones on high risk and will likely result in more of these gadgets getting infected. Therefore, both the general populace and businesses are targeted. This implies that even end-users who are bound to download COVID-19-related applications are also being tricked into downloading ransomware as it appears as one of the modern legitimate applications. In addition, the functioning of many security teams at organisations is likely to be impaired because of the COVID-19 pandemic, which impairs the detection abilities of malicious activities.

In South Africa, the enforcement of the 'work from home' policy by some companies has become popular. Thus, it is plausible to learn that a stable power supply and a fast internet connection may be a luxury in some rural areas, and this may force employees and students to work from public spaces or internet café's to utilise power and free internet facilities.[8] Notwithstanding a milestone achievement made by the South African government in making sure that affordable data are available to students to work online, this move would expose the computing facilities and confidential information of institutions to theft or damage.

The problem is that employees lack the knowledge concerning the risk associated with social media platforms for the computing facilities and confidential information of their institution, especially when used at the workplace. Some organisations have not effectively established information security awareness programmes for their employees, which can result in unintentional negative behaviour.[9]

Unintentionally, uninformed employees make naïve mistakes that can open the door to cyberattacks that exploit vulnerabilities in the organisation's system of controls. Moreover, if employees are not well informed regarding the risks and privacy issues when accessing social media during working hours at the workplace, they could expose the organisation's reputational damage and customer loss.[4,5] Furthermore, the emergence of COVID-19 plague has forced businesses and governments to depend increasingly on technology to assist citizens, thus the use of digital systems have become popular and the only alternative to save people and businesses.[8] New demands have been placed on networks and datacentre infrastructure as remote working and collaboration tools have become important systems, with a new wave of demands placed on networks and datacentre infrastructure.[10] The emergence of malicious actors in a bid to exploit fears over the pandemic has placed many organisations to panic and they have extended networks beyond the firewall as security remains a pervasive concern.[8]

This study aims to propose a model to ensure employee information security compliance when using social media for work-related business. To achieve this objective, a desktop literature review was conducted to identify risks involved when using social media in the workplace and any work-related business. The structure of the study is outlined as follows: literature is discussed in the first section followed by a theoretical foundation applied in this research. Other sections to follow are comprised of information security awareness, compliance strategies and thereafter, a proposed model for the study and the conclusion.

Literature review

The literature review highlights relevant topics of the study.

Social media use and human firewall

According to Tarantino, McDonough and Hua,[11] social media refers to websites and applications that enable organisations to create and share information. These include Twitter, MySpace, Facebook, Flickr, Google Plus and YouTube.[9] The use of social media and its adoption in organisations has increased as the benefits are substantial. Various studies state that marketing is the biggest beneficiary of social networking tools.[9,12] Organisations encourage employees, especially in the sales and marketing department, to reach out to customers using social media as most customers use these platforms to search for goods and services.[12,13] Social media use has the potential to increase sales and market-share for organisations. In addition, social media use at the workplace can help organisations to maintain a competitive advantage, and some use it as a communication tool to spread messages faster amongst core workers and customers.[13,14]

Schraner[15] adds that interacting with customers on social media sites helps the organisation understand customer needs much better and improve service delivery. Engaging with consumers helps to discover undelivered consumer demands and complaints. Furthermore, allowing employees to make use of social media tools is considered helpful on strengthening customer relationships and penetrating new geographical areas, which makes social media tools a key mechanism for sparking innovation.[15] Another possible aspect is that forbidding social media tools in the workplace may harm employee morale and affordable communication.[16]

It is believed that there is no single technology solution that can assist in fighting today's most urgent security problems.[17] Organisations should not just invest in security technology, but also activate a security-conscious workplace culture (human firewall). Human firewall's main objective is to stimulate the awareness of employees to such an extent that they act as a solid line of defence against external attacks that threatens security systems.[4,5,17] A human firewall aims to equip employees and block weakest links

in the organisational security by educating employees about the security of the organisation. There are three main components of human firewall: employee education, minimising human error and getting ahead of new threats.

Employee education

Security education should cover all levels within the organisation and should go beyond treating security training as compliance-based 'check-box' activity.[1] Information technology (IT) departments are not spared. They need education on how to implement policies that are secure but not too restrictive that the flow of business is disrupted. Administrators have become the de facto target for attacks, as they allow an easy pivot point to gain access inside the network. Hence, IT departments are more vulnerable because of elevated administrative privileges on the network, as well as weaker controls for email attachments and internet browsing.

Minimising human error

Hackers and spammers usually predict human nature to exploit human error-related opportunities. They do so by using social engineering to gain trust by manipulating vulnerable users into clicking on malicious links in emails that are thought to be from legitimate sources.[18] This common trickery known as phishing requires the user to be complicit in by clicking the link. Hence, the most reliable defence is educating employees about possible threats. To counter this popular attack, there is a range of new technologies helping organisations to deal with these threats. For instance, sophisticated email gateways are used through creation of unique safe links in every email hyperlink before it reaches the user's inbox. To counter a situation where some employees invariably click bad links, there is a need for an added layer of protection which helps to protect users who either intentionally or accidentally fail to follow training and guidance.[19]

New threats

There is a need for employees to be well informed and adapt to the latest security measures as new threats, like phishing and malware change constantly.[20] In a recent report by Panda Security[21] (February 2020), it is said that, in a total of about 30 million unique new threats recorded every day, an average of 82 000 are new malware strains.[2] With such rapid increment of new attacks, smart security investments cannot rely on yesterday's 'tried and true' methods to stay ahead of the game.

Traditional firewall

A traditional firewall can be defined as a device that can control the traffic that is allowed to enter or exit a point within the network. It is comprised of both hardware and software meant to protect computers from hackers and other threats. It blocks dangerous software or data from reaching the system.[5] Hardware firewalls provide network-wide protection to fight online threats. Software firewalls installed on individual computers are meant to inspect data more closely and blocks specific programmes from sending data to the internet. A combination of both kinds of firewalls is sometimes used to provide a more complete safety net for networks with high-security concerns.[17]

Hardware firewalls

A hardware firewall is installed between the internet and a local area network (LAN) of computers.[2] Inspection of all the data received from the internet is done, passing along the safe data packets whilst blocking the potentially dangerous packets. Hardware firewalls may require expert set up to properly protect a LAN without affecting the performance and access to remote sites or web pages and this may not be a feasible solution in the absence of a dedicated IT department. To simplify the job, for businesses with many computers, network security should be controlled from one single device.[17]

Software firewall

Software firewall is usually installed on individual computers on a network.[20] Software firewalls are not similar to hardware firewalls, as the latter could easily distinguish between programs on a computer. It can allow or block the execution of various programs and allow data to one program whilst blocking another.[1] Software firewalls also filter outgoing data and remote responses to outgoing requests. However, it is also important to note that software firewalls require installation, updating and administration on each computer.[22]

Theoretical foundation

This study utilised a desktop literature review method. Deterrence theory and the theory of reasoned action (TRA) were employed as a theoretical foundation as they are widely used information systems theory. Theory of reasoned action explores the relationship between behaviours and attitudes within human action. It is useful on predicting how individuals will behave by analysing their pre-existing attitudes and behavioural intentions. Theory of reasoned action depicts a model containing benefits for forecasting the intention to perform a behaviour based on an individual's attitude and normative beliefs.[4,5] It evaluates two incentive components, the attitude and subjective norms.

The theory proposes that an employee's behaviour intention depends on both subjective norms and attitude. The theory explains that an employee's attitude towards information security influences the individual's behaviour. It is determined by intent, a basis to execute a certain behaviour.[4,5,23] In addition, TRA relies on the notion that employees make realistic decisions based on the information available to them. Employees who make naïve mistakes and those with a negative attitude towards information security at organisations require motivation to comply for them to

behave responsibly. An awareness programme is therefore needed to educate and train them to protect the organisation's information assets.[4,5]

This study applied the deterrence theory (DT) to threaten or explain the consequences of failure to behave responsibly when using social media. Deterrence is described as a threat of punishment to employees through some form of sanction.[24] Similarly, DT is the idea that a more severe punishment will more likely deter a rationally calculating human being from committing unjust acts. Deterrence can be classified into two categories: specific and general. The difference between these two is that the latter refers to the actual punishment of an individual offender, whilst the former denotes the implications of the threat of punishment and that threat involves both the risk of the harshness of the sanction and detection. Elliott[25] adds that the DT can be applied as a preventive control and has various effects including intimidation, education and reinforcement. The intimidating effects of punishment are general and specific. Furthermore, the DT can be used as a formal sanction to stimulate and reinforce employees to behave more responsibly when using social media at the workplace. If employees do not withdraw from illegal activities on social media out of fear of the negative costs, they are not deterred. However, there are some limitations to the DT. Elliott[25] points out that DT has less impact in controlling or getting read of habitual, unthinking behaviour from the employees because of heuristic information processing.

Research methodology

The study employed a scoping literature review to gather data. Literature analysis was carried out based on the information obtained from Google Scholar, Science Direct, as well as Research Gate and the Association for Computing Machinery (ACM). Research was undertaken thoroughly from the chosen sources to confirm the authenticity of every article relevant to the study and meeting all the inclusion criteria.[25] The search was done extensively to gather relevant data from every article that corresponded to the inclusion criteria irrespective of the kind of studies they were derived from. All available articles were included as long as they have touched the risks involved when using social media in the workplace. Whilst incorporating relevant information within the parameters, articles that were published between 2010 and 2018 were consulted, respectively (Table 1).

The research has made use of a forward and backward search strategy to ensure inclusion of relevant references in the review (Table 1). An extensive database was compiled of the keywords that were used in the search process. This included a full description of the keywords and the motives for inclusion of these various keywords. Table 1 illustrate the format used to compile keywords used to download the article from the database. The complete articles were derived from the numerous databases and analysed individually by two academics. Thereafter, the researchers reached agreement by coordinating their findings to identify the articles, which are relevant for the study.

It was challenging to utilise any special tool in the data extraction process because the articles to be analysed were based on various types of studies. Therefore, extraction and tabulation of data were done manually and separately before comparing and combining it.[26] Findings were synthesised into more relevant data after grouping the findings under each theme (Figure 1). Reciprocal translation analysis was used. After a comparison of findings of one study, similarities were drawn from there and the synthesised outcome was then compared with another study until all articles had

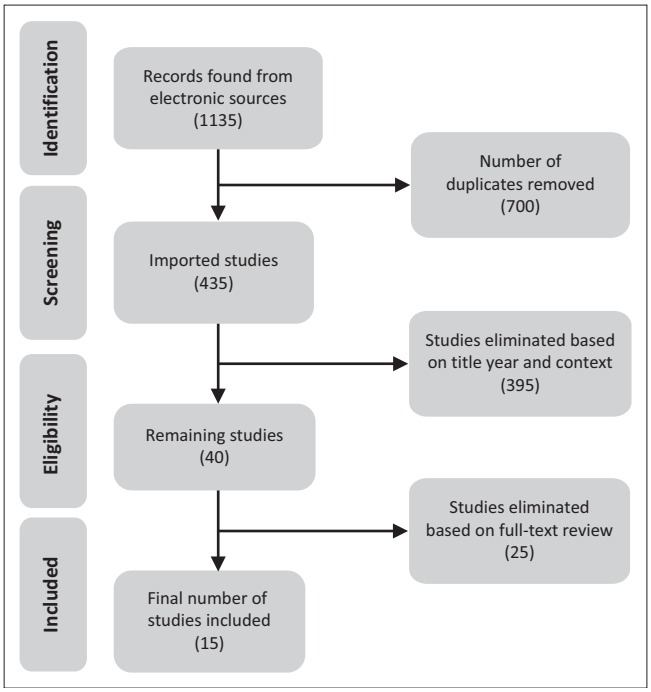

FIGURE 1: Preferred reporting items for systematic reviews and meta-analysis model employed in the study, modified after Boell and Cecez-Kecmanovic.[26]

TABLE 1: Keywords used for the database extract after Boell and Cecez-Kecmanovic.[26]

Search phrase	Reason for modifying	Number of articles
Social media	The original phrase used to search all database	4 500 000
Social media + risks	Used to refine the search results to only include articles that focus on social media risks	3 060 000
Social media + risks + employees	Used to refine the search results to only include articles that focus on the risks associated with employees at the workplace	1 130 000
Social media + risks + employees + workplace	Used to refine the search results to only include articles that focus on the risks associated with employees at the workplace	17 800
Social media + risks + employees + workplace + South Africa	Used to refine the search results to only include articles that focus on the risks associated with employees at the workplace in South Africa	22 700
Social media + risks + in Africa/(name of the African Country)	Used to refine the search results to only include articles that focus on the risks associated with employees at the workplace in African countries such as Nigeria, Kenya and Ghana	14 600

been synthesised (Figure 1). Literature analysis results were grouped into the three categories of factors as outlined by the theoretical background. In Figure 1, the Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA) model, employed in this study is shown in Figure 1.

The inclusion criteria contained within is that the study must address risks associated with social media use at the workplace. This was carried out to allow numerous studies to be involved and to take part in the review process. A total of 1135 studies of journal articles and conference articles from all the databases were obtained. These results have included both unsuitable and unfiltered data. To filter the results, search engine filtering, range and regional filtering were used and resulted in 435 studies remaining. In order to analyse suitability, these studies were again read and screened, based on the exclusion criteria as follows: published between 2010 and 2018 and whether the studies addressed risks associated with social media use at the workplace.

After the first screening, 435 studies were obtained. The full text of these studies was reviewed by the authors and only 15 studies were retained. The reasons for the elimination of 420 studies were:

- A total of 395 studies were eliminated because of the title, year and context.
- The other 25 studies did not discuss the challenges associated with social media when used in the workplace.
- Table 1-A1 lists the 15 studies that are included in the research and the identified topics from after the thematic analysis.

Results

Employees should be made aware of the risks of using social media and securing information assets, as well as the associated costs if this is not done correctly.[18,20] Many employees are vulnerable and are targeted by cybercriminals.[5] Whilst there are many reasons for employee vulnerability, the primary factor is that employees lack adequate knowledge on the risks involved when using social media and often find themselves wandering into cyberspace without any awareness preparation.[23] Sophos[27] stated that malware and attack vectors are targeting social media users as they lack knowledge about them and securing information. Some employees access links, adverts and pop-ups that infect their machines, which allows access to criminals who cause harm to organisations.[28] Van Niekerk and Maharaj[16] provided an example of cyber-threats and malicious emails distributed through Facebook by the Pushdo botnet malware distributor. In another example, employees were tricked by malware named Koobface into clicking on a link affected by Trojans that hijacked their Web browser. An organisation must have an awareness campaign about security controls such as firewalls and antiviruses that can be used to minimise threats from malicious software.[16]

Social media can build or damage the reputation of an organisation. Van Niekerk and Maharaj[16] stated the challenge to contain the released information that can be harmful when it is on social media. An employee caused damage to the organisation using social media. A former worker of the Good Guys, posted aggressive, threatening material on his Facebook page about the organisation as he was frustrated by not been paid his commission. A further case was decided in 2008 where some of the cabin crew members of Virgin Atlantic posted on Facebook taunting remarks about Virgin's fleet and passengers. One post claimed that there were cockroaches in the planes and another labelled a traveller as 'smelly and annoying'. This brought the company in disrespect and the crew members were sacked.

The same holds true for Twitter™. In 2015, an employee was dismissed from a communications director post of the New York-based internet empire InterActive Corp for having tweeted a puerile post that linked Acquired Immunodeficiency Syndrome (AIDS) with race. This is an example of the 'authority' of Twitter and how this platform can destroy individuals who offend or abuse the rights of others on social media.

Studies assert that social media can increase the prevalence of abuse and cyberbullying.[16,29] Li[29] defined cyberbullying as:

> [*A*]n attack which may be verbal, physical, makes obscene gestures or intentionally isolates another person from a social group and it occurs on social networking sites where employees could be harassed with harmful text or images. (p. 371)

Thus, social media can be viewed as a source of malicious behaviour in the workplace. At Fair Work Australia an employee posted on her account (MySpace) threatening messages and described how she was sexually harassed by her employer and the employee refused to remove the post.

Another risk is when personal accounts are used to communicate work-related information, which may result to the unauthorised disclosure of confidential information. In a recent case, Hillary Clinton used her private email server for State communication, which resulted in leaking party secrets to the opposition parties.[30] Similarly, leaking trade secrets through emerging technologies has severe effects as an organisation can suffer financial loss and decreased market share.[20,31] An employee such as these needs to be trained to enhance their knowledge concerning the use of information confidentiality.

Most organisations hold confidential and sensitive client information, which can be disclosed accidentally. Hicks[18] provided an example of a nurse who posted a medical record of a patient, including admission date and her full name on his Facebook page. Such an employee needs to be trained to enhance his or her knowledge concerning the use of information confidentiality. Illegal access, as well as the use of confidential information found on an employee social media profile, may perhaps lead to numerous risks, for instance, identity theft, fraud, stalking and loss of employment.[22,32] For example, an employer found an

employee who was pregnant and her working hours were shortened. The employee realised that the employer found this information on her Facebook page. There is a need to educate employees about privacy preservation online.[32]

Furthermore, Shullich[3] added that there is an increasing number of dismissal cases as organisations punish offenders to serve as an example to other employees to behave responsibly. Van Niekerk and Maharaj[16] provided an example where a worker was dismissed because the company's guidebook warned workers not to insult and threaten other employees on social media as it is grounds for dismissal. Williams[33] provided an example of eight workers who lost their jobs after an insane social media post.

Some organisations are prohibiting workers from using social media in the workplace as a measure to combat abuse of social media tools. Bolotaeva and Cata[31] indicated that certain employees spend too many hours on social networks doing non-work related activities, which harms productivity, results in network utilisation issues and increased risk of exposure to malicious software. Hence, there is a need for monitoring of employees' actions and implementing policies that discourage the misuse of social media tools when employees are at the workplace.[34] It is thus essential to increase the knowledge of employees regarding social media risks through awareness programmes.

Managerial implications

The study suggests that employees need to be educated concerning human and traditional firewalls. This can be achieved through security awareness programmes. Compliance strategies should be implemented to get rid of social media-related risks, whilst enjoying the benefits of using these powerful platforms. Hence, integrity, confidentiality and availability of information in organisations are preserved and promoted.

Information security awareness programmes

Information security awareness programmes help to educate employees in the organisation concerning cyber-attacks. Awareness is not the same as training: it is a method of stimulating, motivating and reminding employees what is expected of them.[35] Gundu et al.[23] found that information security awareness aims at raising employee's knowledge towards securing organisational assets. Besides, information security awareness programmes explain what will happen to an organisation and employees if information security management fails to inspire a workforce to take security seriously.[36]

Implementing successful security awareness programmes is an essential step in enhancing information security within organisations. Aloul[4] and Ajzen and Fishbein[5] stated that security awareness provides the workforce with the knowledge that they need to behave responsibly and assists to reduce social networking risk in organisations. It is imperative to know that employees need access to training on information security awareness.[5,20] Programmes on information security awareness communicate security standard information to the workforce, which helps to change negative attitudes towards information security.[34] However, steering security awareness programmes in organisations are fruitless if employees do not act on them or follow the information received during the awareness campaigns.[6,37] Various methods can be used to convey a security message to employees. These strategies include classroom-style training, security awareness websites, security posters, booklets and newsletters. The following section discusses components for mitigating social media risk.

Compliance strategies

There are actions that organisations can use to reduce social media risk to acceptable levels. These elements include security policies, social media guidelines and punishment to educate employees on how to behave when using social media tools.

Security policies

Kentucky University[38] mentioned that social media policy explains what the employees must not do on social media sites in the course of their employment. Policies on social media determine the guidelines and clearly define the standards of satisfactory behaviour that organisations expect from the workers when using social media tools.[35] Social media policy provides relevant guidelines that limit the freedom of workers when interacting with customers online.[5,20]

A well-designed and thorough policy on social media use can minimise social networking risks.[32] Social media policy addresses various risks such as disclosure of organisation information, harassment and discrimination on social networks. In addition, when organisations take proper steps to address social media vulnerabilities, they can successfully safeguard valuable information and mitigate legal actions.[38] Organisations have social media usage policies but these guidelines are not implemented because they are not enforced by top management.[3] There is a need for top management to administer social media and privacy policies to reduce the risk inherent to these technologies. These policies need to be in place and well explained to the employees who often make naïve mistakes. Accordingly, employees need to be trained on safe social media practices in concert with a social media policy as it helps to mitigate social media risks.[28]

Social media guidelines

Organisations' use of social media policy will help to educate employees about opportunities and the risk social

media present when accessed and used at the workplace.[12] Social media guidelines provide employees with relevant guidance for using social network tools to communicate work-related business. Besides, they assist in clarifying business and personal use of social media.[33]

Punishment

Punishment is explained by the DT and is another enforcement strategy that organisations can employ.[24] This involves imparting fear to malicious employees such that others will be aware of the punishment. This enforcement strategy can be used in organisations and functions as an example for employees who have not yet participated in criminal events. The following section will introduce the proposed model of implementation.

Proposed model

Figure 2 depicts the proposed model, which aims at addressing risks, associated with social media. Cyber breaches by employees expose the organisation's 'trade secrets', which could lead to financial, customer loss and reputational damage. To address social media risk, an information security awareness strategy needs to be in place to educate employees about information security controls; how to behave when using social sites and the implications of not obeying the social media policy.

The first subsystem of the model (Figure 2) consists of education, training, CIA and privacy. All four components are needed to make sure that social media risks are minimised to acceptable levels. If employees are well informed through awareness strategies (education and training) about the need to maintain CIA and privacy of information as it assists in achieving employee information security compliance, which is cultivated through policies, procedures and best practices. The second subsystem (Figure 2) is an enforcement approach and consists of a punishment component. If some components of the two subsystems are absent, then output (reducing social media risks) will not be cultivated. The proposed information security awareness model is presented here.

The proposed model includes components from the Reasoned Action Theory, the DT (punishment), the CIA and privacy. Theory of reasoned action describes the constructs that influence employee behaviour. Theory of reasoned action relies on the belief that employees make realistic decisions based on the information available to them and awareness strategies, education and training could be used to provide information regarding social media risk. Naïve employees could be able to behave responsibly if they are trained about social media risks.[4,5] The DT defines the benefits derived from using punishment (e.g. dismissal) in the case that an employee has violated the social media policy. This will serve as an example and a warning to every employee.

Thereafter, an awareness will be present amongst employees of the consequences by not following security policies available in the organisations.[24] The model demonstrates how awareness strategies (training and education), privacy and CIA can be employed to guide employee information security compliance to ensure that social media risk is minimised.[5,20]

Conclusion

Actions of employees could increase the prevalence of cyber risk in various organisations. It can be through

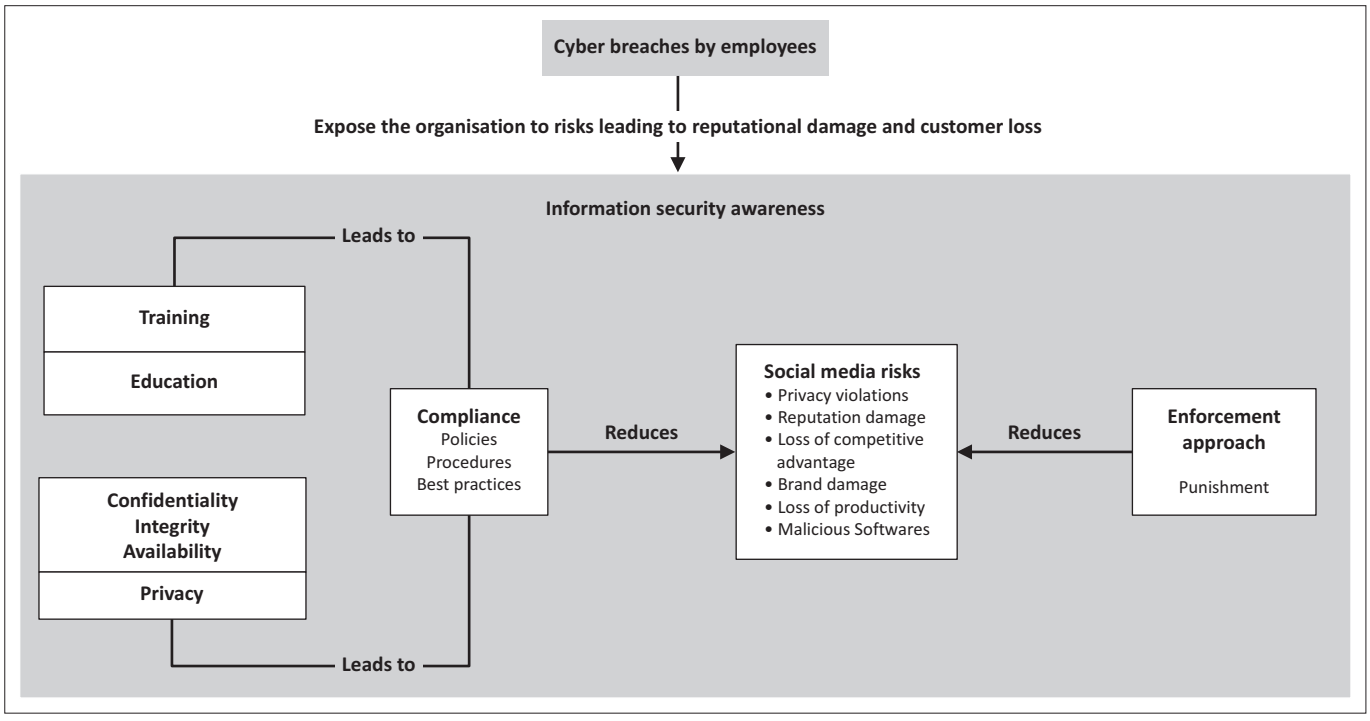

FIGURE 2: Information security awareness model.

careless handling of sensitive data, exposure to phishing attacks, weak passwords, or data breaches caused by user awareness issues. Cyber breaches by employees can open the door to cyberattacks that exploit vulnerabilities in the organisation's system of controls and expose the organisation to risks leading to reputational damage and customer loss. Although these technologies such as social media have become essential to organisations, especially now during the COVID-19 pandemic, it is essential to negate cyber breaches.

Organisations need to establish information security control awareness programmes to enhance the level of security and educating employees on how to behave when using social media tools both at work or at home. The study recommends that the implementation of the various aspects discussed in the proposed model of information security awareness will contribute towards minimising social media risks to acceptable levels, whilst enjoying the benefits of using these powerful platforms. Moreover, this will ensure that CIA and privacy of information in organisations are preserved.

Acknowledgements

The authors wish to acknowledge Rhodes University and Walter Sisulu University for their support.

Competing interests

The authors declare that they have no financial or personal relationships that may have inappropriately influenced them in writing this research article.

Authors' contributions

O.T.M. assisted in study design, acquisition, analysis and interpretation of data. O.T.M., S.F.D., K.S. and C.J.S.F. were involved in drafting of manuscript and critical revisions.

Ethical consideration

This article followed all ethical standards for research.

Funding information

This research received no specific grant from any funding agency in the public, commercial or not-for-profit sectors.

Data availability

The authors confirm that the data supporting the findings of this study are available within the article.

Disclaimer

The views and opinions expressed in this article are those of the authors and do not necessarily reflect the official policy or position of any affiliated agency of the authors.

References

1. Moletsane T, Tsibolane P. Mobile information security awareness among students in higher education. Information Communication Technology and Society Conference. Durban: Durban University of Technology; 2020. pp. 12–17.
2. Van Der Walt E, Eloff J, Grobler J. Cyber-security: Identity deception detection on social media platforms. Comput Secur. 2018;78:76–89. https://doi.org/10.1016/j.cose.2018.05.015
3. Shullich R. Risk assessment of social media [homepage on the Internet]. SANS Institute InfoSec Reading Room; 2011 [cited 2020 April]. Available from: http://www.sans.org/reading-room/whitepapers/privacy/risk-assessment-social-media-33940
4. Aloul FA. The need for effective information security awareness. J Adv Inform Tech. 2012;3(3):1–7. https://doi.org/10.4304/jait.3.3.176-183
5. Ajzen I, Fishbein M. Understanding attitudes and predicting social behaviour. Englewood Cliffs, NJ: Prentice-Hall, 1980; p. 278.
6. Frauenstein E, Flowerday S. Social network phishing: Becoming habituated to clicks and ignorant to threats? Information Security for South Africa [homepage on the Internet]. Johannesburg: Institute of Electrical and Electronics Engineers, 2016 [cited 2020 April]; pp. 98–105. Available from: https://ieeexplore.ieee.org/document/7802935
7. SANS. Security awareness compliance requirements. Securing the Human [homepage on the Internet]. 2015 [cited 2020 May]; pp. 1–6. Available from: http://pikitdigital.net/material/interes/SANS_Security_Awareness_Report_2015.pdf
8. Bhadada P, Yousuf Z. Technology trends that will shape the post-COVID era [homepage on the Internet]. 2020, April 14 [cited 2020 May]. Available from: https://zinnov.com/role-of-technology-in-the-fight-against-covid19
9. Batikas M, Bavel R, Martin A, Maghiros I. Use of social media by European SMEs [homepage on the Internet]. 2013 [cited 2020 March]. Available from: http://www.europski-fondovi.eu/sites/default/files/dokumenti/KK0113565ENN_002.pdf
10. Cascio W, Montealegre R. How technology is changing work and organizations. Annu Rev Organ Psychol Organ Behav [serial online]. 2016 [cited May 2020];3:349–375. Available from: https://www.annualreviews.org. https://doi.org/10.1146/annurev-orgpsych-041015-062352
11. Tarantino K, McDonough J, Hua M. Effects of student engagement with social media on student learning: A review of literature [homepage on the Internet]. 2013; pp. 1–14. Available from: http://studentaffairs.com/ejournal/Summer_2013/EffectsOfStudentEngagementWithSocialMedia.html
12. Cilliers L, Chinyamurindi W, Viljoen K. Factors influencing the intention to use social media for work-related purposes at a South African higher education institution. SA J Hum Resour Manag. 2017;15:1–11. https://doi.org/10.4102/sajhrm.v15i0.859
13. Kaplan A, Haenlein M. Users of the world, unite! The challenges and opportunities of social media. Bus Horiz. 2010;53(1):59–68. https://doi.org/10.1016/j.bushor.2009.09.003
14. Changqing H, Jibao G, Wei W, Xuesong Z, Jun S. Social media use in the career development of graduate students: The mediating role of internship effectiveness and the moderating role of Zhongyong. High Educ. 2017;74(6):1–20. https://doi.org/10.1007/s10734-016-0107-8
15. Schraner L. Explore the benefits of social media for small and medium enterprises (SMEs) [homepage on the Internet]. 2012 [cited April 2020]. Available from: http://www.socialabacus.com/explore-the-benefits-of-social-media-for-small-and-medium-enterprises-smes
16. Van Niekerk B, Maharaj M. Social media and information conflict. Int J Comm. 2013;7:1162–1184.
17. Scott-Cowley O. The 'human firewall': A more proactive approach to infosec [homepage on the Internet]. 2014 [cited May 2020] Aug 19. Available from: https://www.scmagazine.com/home/sc-marketscope/messaging-security-resource-center/the-human-firewall-a-more-proactive-approach-to-infosec
18. Hicks J. Social media's role in privacy breaches [homepage on the Internet]. 2016 [cited May 2020]. Available from: http://medicaloffice.about.com/od/privacyandsecurity/a/Social-Medias-Role-In-Privacy-Breaches.htm
19. Perkins J. Policy-information security policy. Lond Sch Econ Polit Sci. 2016;3(13):1–11.
20. Chetty P, Law C. The top 5 intellectual property risks on social media [homepage on the Internet]. 2014 [cited May 2020]. Available from: https://smetoolkit.businesspartners.co.za/en/content/top-5-intellectual-property-risks-social-media
21. Panda Security. 2020 State of Malware Report. Burlington, MA: Panda Security, 2020; p. 57.
22. Mainier MJ, Louch MO. Online social networks and the privacy paradox: A research framework. Issue Info Syst. 2010;6(1):513–517.
23. Gundu T, Flowerday SV. Ignorance to awareness: Towards an information security awareness process. SA Inst Electr Eng. 2013;104(2):69–79. https://doi.org/10.23919/SAIEE.2013.8531867
24. South D. General deterrence and behaviour change: A comment on the Australian psychological society position paper on punishment and behaviour change. Aust Psychol. 1998;33(1):76–80. https://doi.org/10.1080/00050069808257269
25. Elliott B. An analysis of risk and deterrence: Background for LTSA review of administrative penalties in New Zealand, Land Transport Safety Authority. 2003;1:232.
26. Boell SK, Cecez-Kecmanovic D. A Hermeneutic approach for conducting literature reviews and literature searches. Communications of the Association for Information Systems. Atlanta, GA: Ais ELibrary, 2014; p. 34.

27. Sophos Boston. Sophos security threat report [homepage on the Internet]. 2013 [cited May 2020]. Available from: https://nakedsecurity.sophos.com/2012/12/04/sophos-security-threat-report
28. Waxer C. CIOs struggle with social medias security risks [homepage on the Internet]. 2011 [cited May 2020]. Available from: http://www.govtech.com/pcio/CIOs-Social-Media-Security-Risks-021111.html
29. Li Q. Cyberbullying in high schools: A study of students' behaviours and beliefs about this new phenomenon. J Aggress Maltreatment Trauma. 2010;19(4):372–392. https://doi.org/10.1080/10926771003788979
30. Myers SL, Lichtblau E. Politics: Hillary Clinton is criticised for private emails in State Dept. Review [homepage on the Internet]. The New York Times. 2016 [cited May 2020] Nov 8. Available from: http://www.nytimes.com/2016/05/26/us/politics/state-department-hillary-clinton-emails.html
31. Bolotaeva V, Cata T. Marketing opportunities with social networks. J Internet Soc Netw Virtual Communities. 2011;1:1–8. https://doi.org/10.5171/2011.409860
32. Torten R, Reaiche C, Boyle S. The impact of security awareness on information technology professionals' behavior. Comput Secur. 2018;79:68–79. https://doi.org/10.1016/j.cose.2018.08.007
33. Williams V. 8 insane social media posts that got people fired [homepage on the Internet]. 2015 [cited April 2020]. Available from: http://www.oxygen.com/very-real/8-insane-social-media-posts-that-got-people-fired
34. Harvard University. Guideline for using social media. Guidelines & best practices [homepage on the Internet]. Version 2.0, 2014 [cited April 2020]; p. 9. Available from: https://provost.harvard.edu/files/provost/files/social_media_guidelines_vers_2_0_eff_081814.pdf
35. Winkler I, Manke S. 7 reasons for security awareness failure [homepage on the Internet]. 2013 [cited May 2020]. Available from: http://www.csoonline.com/article/736159/7-reasons-for-security-awareness-failure
36. Ngoqo B, Flowerday S. Information security behaviour profiling framework (ISBPF) for student mobile phone users. Comput Secur. 2015;53:132–142. https://doi.org/10.1016/j.cose.2015.05.011
37. Pepper C. Security awareness training evolution. Securosis. 2013;1(5):1–18.
38. Kentucky University. Social media policies and guidelines. Admin Regul. 2011;10(4):1–5.
39. Whitman ME, Mattord HJ. Principles of information security. 4th edn [homepage on the Internet]. Boston, MA: Cengage Learning; 2012 [cited May 2020]. Available from: www.cengage.com
40. Kritzinger E, Von Solms SH. Cyber security for home users: A new way of protection through awareness enforcement. Comput Secur. 2010;29:840–847.
41. Clark LA, Roberts SJ. Employer's use of social networking sites: A socially irresponsible practice. J Bus Ethics 2010;95:507–525. https://doi.org/10.1007/s10551-010-0436-y

Appendix starts on the next page →

Appendix 1: Studies that are included in this research.

TABLE 1-A1: List of 15 studies that are included in the research and the identified topics after the thematic analysis.

Number	Author	Title	Year
1	Aloul[4]	The need for effective information security awareness. Journal of advances in information technology.	2012
2	Chetty and Law[20]	The top five intellectual property risks on social media	2014
3	Gundu et al.[23]	Ignorance of awareness: Towards an information security awareness process. South African Institute of Electrical Engineers	2013
4	Hicks[18]	Social media's role in privacy breaches.	2016
5	Kentucky University[38]	Social media policies and guidelines	2011
6	Kritzinger and Von Solms[40]	Cybersecurity for home users: A new way of protection through awareness enforcement.	2010
7	Clark and Roberts[41]	Employer's use of social networking sites: A socially irresponsible practice	2010
8	Pepper[37]	Security awareness training evolution	2013
9	Perkins[19]	Policy-information security policy	2016
10	SANS[6]	Security awareness compliance requirements. Securing the human	2015
11	Sophos[27]	Sophos security threat report.	2013
12	Van Niekerk and Maharaj[16]	Social media and information conflict. International journal of communication.	2013
13	Waxer[28]	CIOs struggle with social's security risks	2011
14	Whitman and Mattord[39]	Principles of information security. Boston: Cengage Learning.	2012
15	Winkler and Manke[34]	Reasons for security awareness failure	2013