INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Published Online: 05 February 2023 Vol 13, Issue 2, (2023) E-ISSN: 2222-6990

The Impact of Social Media Usage on the Organisation's Reputation Risk through its Cybersecurity

Fatin Aqilah Maskuri[a], Mohd Zailani Othman[b], Idris Osman[a], Suhailah Kassim[a] and Noraznira Abd Razak[c]

[a]Human Resource Department, Faculty of Business and Management, Universiti Teknologi MARA, Malacca Branch, Malacca City Campus, 75300 Malacca City, Malacca, Malaysia, [b]Management Department, Universiti Teknologi MARA, Malacca Branch, Malacca City Campus, 75300 Malacca City, Malacca, Malaysia, [c]Risk and Insurance Department, Faculty of Business and Management, Universiti Teknologi MARA, Malacca Branch, Alor Gajah Campus, 78000 Alor Gajah, Malacca, Malaysia

Corresponding Author's Email: mzothman@uitm.edu.my

Abstract

The utilisation of social media among organisations is growing tremendously and is seen to be moving forward in line with the rapidly evolving technology in Malaysia. It is inevitable that social media not only provides benefits to organisations but also exposes organisations to various risks. Local organisations often get public attention when an issue related to the organisation goes viral on social media, exposing them to reputation risk and eventually affecting their reputation. Changes in the reputation of organisations affect relationships with their stakeholders. Most organisations today are aware of the importance of using social media. Despite the beneficial usage of social media, organisations encounter social media risks that require attention and must be catered to wisely. Due to the vulnerability of social media, there is a high possibility of being attacked, which indicates the need for effective cybersecurity in organisations. The aim of this conceptual paper is to discuss the relationship between social media usage and organisation's reputation risk, in which organisation's cybersecurity is predictably act as a mediator in the relationship between the variables.

Keywords: Social Media, Cybersecurity, Reputation Risk, Organisations, Stakeholders

Introduction

The rise of social media has led to changes in how organisations operate their daily activities (Olanrewaju et al., 2020). Nowadays, the use of social media is not limited to individuals. Organisations also take the opportunity to leverage social media. The utilisation of social media among organisations is growing tremendously and is seen to be moving forward in line with the rapidly evolving technology in Malaysia. Organisations are now creating social media accounts to improve their social network presence, enhance public interest in their organisations, and connect with the online public (Parveen et al., 2015).

Malaysia is moving in tandem with the 4.0 industrial revolution, where digital technology connects individuals and organisations. Thus, organisations need to follow the same pace to remain relevant. According to Van Osch & Coursaris (2013), organisational social media is a technology that supports various actors, such as management, employees and external stakeholders, in various organisational communication activities. The functions of organisational social media include producing user-generated content, developing and maintaining social relationships, or enabling other computer-mediated interactions and collaborations in a specific organisation and its environment (Van Osch & Coursaris, 2013).

With the advances in technology, these diverse stakeholders can create and curate content and become spectators (McCorkindale & Distaso, 2013). Nowadays, stakeholders often rely on social media to look for information related to the organisations' stories or updates. Benthaus, Risius, & Beck (2016) indicated that it is important to provide relevant content to the respective stakeholders via social media since it has the highest return on the reputation of the organisation. According to Choi & Thoeni (2016), consumers use more of social media as a trusted source of information to give comments on organisations' offerings. It continues to be difficult for organisations to make a strategic decision at the right level of engagement to share the message while improving the stakeholders' perception of the organisation (Benthaus et al., 2016).

Statistics show that in 2017, around 55% of the companies in Malaysia working in the services sector were using social media to publish information about themselves (Muller, 2021). Using social media platforms such as Facebook, YouTube, Twitter, LinkedIn, Instagram, etc., continue to attract people by building online communities to allow people to connect and interact with organisations. It is inevitable that social media not only provides benefits to organisations but also risks need to be encountered. Also, social media is vulnerable to cyberattacks.

Social media not only contributes to the spike in cybersecurity problems but also to the rise of cyberattack threats (Ali et al., 2019). The increase in cyberattacks has made cybersecurity the top concern in organisations (Gibbs, 2020). Thus, cybersecurity is important in organisations, especially involving social media, since it could impact the organisation's reputation. Social media has made cybersecurity threats a primary attention that needs cybersecurity efforts.

Organisations leveraging social media make cybersecurity the top priority to address. Dealing with digital technology, such as utilising social media, necessitates the most effective security to protect the organisation's data and information from being attacked, misused, or taken advantage of by irresponsible parties for their interest. Hence, this study assumes that a good cybersecurity implementation should facilitate organisations to minimise reputation risk, particularly with the utilisation of social media. This paper adds to the body of knowledge regarding the importance of cybersecurity to mitigate an organisation's reputation risk from using social media, which is deemed beneficial to organisations.

This conceptual paper explains the organisation's reputation risk, social media usage, and cybersecurity based on the previous literature. This study discusses the relationship between social media, an organisation's cybersecurity and the impact on organisational reputation risk. This paper also seeks to enrich the existing literature on social media, organisation's cybersecurity and organisational reputation risk.

Organisation Reputation Risk

Social media has made organisations known globally, which will get the world's attention even with a minor incident. Local organisations often get public attention when an issue related to the organisation goes viral on social media, exposing them to reputation risk and eventually affecting their reputation. Incidents reported on social media can result in brand and reputation damage, a primary concern for large and small organisations (Spanier, 2015). Extensive use of social media has bound organisations to take reputational risks that will negatively affect the organisation's goodwill (Mittal, 2015). Social media helps shape or distort an organisation's reputation by spreading truthful or false information (Kaul et al., 2015).

As mentioned in the previous section, using social media has exposed organisations to cybersecurity threats that could impact an organisation's reputation risk. Reputation risk is one of the key business activities organisations need to deal with (Hövener & Risk, 2015). It is an increasingly important concern in today's business world (Cho & Wu, 2014), especially in well-known and established organisations. The results published by Deloitte (2014) global survey on reputation risk showed that reputation risk is still a "strategic business issue" since most of the executives (eighty-eight per cent) said that it was "a key business challenge" in 2014 (Deloitte, 2014). Reputation risk is a possible cause of threats or damage done to an organization (Soprano et al., 2010), and it can happen in any situation regardless of type of organisation.

Reputation risk comes from uncontrollable external and internal organisational factors (Aula & Mantere, 2013). For example, through electronic word-of-mouth (eWOM), information can be manipulated and reach a larger audience in a split second. It could be a positive, negative or neutral eWOM that can spread rapidly (Majchrzak et al., 2013) and affect an organisation's reputation. Thus, social media has changed how organisations perform their activities and communicate with their stakeholders (Aguenza et al., 2012). Consequently, organisations must be attentive to what the stakeholders mention about them in social media.

Cybersecurity issues could impact an organisation's reputation (Ursillo & Arnold, 2019), while at the same time, the cybersecurity function can help to mitigate cybersecurity threats (Pienta et al., 2020). Cyberattacks can ruin an organisation's reputation (Perera et al., 2022). Organisations must focus on cybersecurity to reduce the reputation risk due to the escalation of cyberattacks with regard to social media usage (Perera et al., 2022). Cyberattacks and adverse social media could contribute to reputation risk events (Pretty, 2018).

Inappropriate use of social media has increased risks to an organisation's reputation, threatens long-term survival and requires management of such reputational risk (Mittal, 2015). Spanier (2015) defines reputational risk as a situation that reduces the stakeholders' perception of an organisation. Reputation risk also refers to a potential event that harms the perceptions of stakeholders and other societal interest or issue groups and, as such, will lead to diminished collaboration and support (Heil, 2018). Reputation risks have been listed on a list of business risks that organisations must take seriously (Aula, 2010). According to Heil (2018), reputational risk is a significant concern among most risk managers because reputation is considered a major source of competitive advantage.

Changes in the reputation of organisations affect relationships with their stakeholders (Lange & Lee, 2011). Consequently, there will be a loss of public trust and customer confidence, which will damage the organisational reputation. Hausmann & Williams (2014) figured out a risk chain to show how social media lead to an organisation's reputational damage. The risk chain example started with the hacking attack by external individuals or groups on the

organisation's social media account, which triggered a loss of content control involving the posting of unauthorised messages or information resulting in the loss of customer confidence and trust manifests in reputational damage.

Social Media Usage

Social media refers to a group of internet-based applications that build on the ideological and technological foundations of Web 2.0 and allow the creation and exchange of User Generated Content (Kaplan & Haenlein, 2010). Organisations commonly use Facebook and Twitter, followed by blogs and YouTube (Parveen et al., 2015). This paper will use the term social media, which refers to the country's social media commonly used by organisations such as Facebook, Twitter, LinkedIn and Instagram.

The use of social media varies according to the needs of the organisation. Most organisations today are aware of the importance of using social media. Leveraging social media in the right way provides many benefits to organisations. Social media possess beneficial usage to organisations such as the fastest medium to get information, a medium for marketing strategies, recruitment, connecting organisations and customers, sharing information to the public, and communicating crisis information to stakeholders information (Reuter et al., 2016; Kapoor et al., 2018; Sivertzen et al., 2013; Parveen et al., 2015; Tajudeen et al., 2018; Horn et al., 2015).

Social media is the fastest medium to get information. It helps organisations receive information from customers, the public, and competitors in the industry (De Lange et al., 2008). Today, organisations use social media for various purposes, such as finding information about their market, customers, and competitors. They leverage social media to identify current trends in the market and their target groups to meet the needs and wants of the customers (Parveen et al., 2015). They also look for information related to their competitors on social media about their movement, tactics and promotional activities that can be treated as a benchmark. According to Wilson (2009), most organisations nowadays act wisely, taking the opportunities through social media to find new business opportunities, new groups of like-minded individuals and organisations, and new sources of industry-specific advice and expertise.

Organisations use social media as a medium for marketing strategies to reach the target market, and it plays a massive role in marketing tactics. Organisations utilise social media for advertising and promoting their services or products. Social media makes it easier for existing or potential customers to get information about their services or products. Social media usage in organisations helps to reduce the cost of marketing activities and customer service (Parveen et al., 2015). Today, most organisations spend their time on social media such as Facebook, Twitter and Instagram, making activities of advertising and promoting products and services on social media to reach many people. Apart from the traditional marketing medium, social media is another option that can attract the attention of netizens and create awareness in Malaysia (Daud & Othman, 2019).

Some organisations use social media for hiring. Despite the traditional ways of advertising job vacancies on traditional media such as television, radio and newspapers, organisations are now shifting their methods of announcing vacant positions by using social media to keep abreast of current technological developments. According to Aguenza et al (2012), using social media for recruitment helps organisations reduce recruiting costs, lessen the number of curriculum vitae generated by the job boards, and impact employee productivity. Social media can expose the organisation's brand to potential employees through recruitment

(Sivertzen et al., 2013). Social media recruiting through platforms such as LinkedIn, Facebook, and Twitter allows organisations to reach a broad candidate pool and sort potential recruits (Cotriss, 2022).

In addition, social media connect organisations and customers. Social media is a platform for customers to share their feedback, comments, and queries, making it easier for the organisation to get instant feedback. On the other side, organisations can quickly and efficiently address customer problems, which can help create a loyal customer base (Cotriss, 2022). With the aid of social media, customers and organisations can build good relationships (Parveen et al., 2015). Social media offers organisations how to respond politely to various reactions whenever customers express their satisfaction or dissatisfaction ranging from experiences, ideas, and knowledge (DeLoach, 2018).

Most organisations use social media to share information about their organisation with the public. The public tends to search for organisations' social media to get information. Hence, organisations that utilise their social media to share information will find ease in discovering the information needed. Social media acts as an information-sharing channel that allows organisations to share products, services, promotions, campaigns, current events and upcoming activities with the public. In addition, social media sites that present the organisation's involvement in corporate responsibility activities provide added value in enhancing the organisation's image (Parveen et al., 2015).

Additionally, organisations can use social media to communicate crisis information to stakeholders. Social media plays a significant role during critical or extreme events to communicate information to stakeholders or the public (Kapoor et al., 2018). Organisations can immediately respond to stakeholder questions and concerns using social media. Through this platform, organisations can understand stakeholders' needs during a crisis and provide further explanations to maintain the organisation's reputation. Roshan et al (2016) reported that most organisations have started using social media to communicate emergencies to their stakeholders. Customers and the public expect organisations to inform about crises quickly via social media. If organisations are slow to respond to a problem, the public and netizens will start spreading negative content and rumours through social media, affecting the organisation's reputation (Roshan et al., 2016). The challenge of using social media for crisis communication is that stakeholders can easily create content, observe the organisation's actions in a crisis and organise activities against the organisation (Gruber et al., 2014; Xia, 2013).

Despite the beneficial usage of social media for organisations, organisations encounter social media risks that require attention and must be catered to wisely. Out of all risks related to social media, organisations are mainly threatened by social media risks such as content, human, and technical risks (Hausmann & Williams, 2014). Social media content can trigger a broad range of risks, such as loss of content control. Social media content is challenging to control since it can be reused, re-purposed, or re-combined, and the content might be unclear (Picazo-Vela et al., 2012; Zerfass et al., 2016). In addition, organisations have less control over the stakeholders' actions on social media (Roshan et al., 2016). Organisational stakeholders consist of customers, suppliers, employees and communities. These stakeholders' actions are beyond the organisation's control, especially on social media, where they can post any good or bad information about the organisation.

Customers can quickly post any dissatisfaction or negative comments publicly on the organisation's social media. Consequently, this will negatively impact the organisation's reputation due to the aggressive action of the customers or clients. Organisational social

media is the most accessible medium for the stakeholders to reach, where they can easily express dissatisfaction and criticise the organisation, especially when there are unexpected issues.

Employees might take advantage of acting more than the authority intended through social media (Rudman, 2011). Employees responsible for managing social media accounts on behalf of the company possibly abuse the given power and trust. This situation can be considered an insider threat. Insider threats refer to a current or former employee, contractor or other business partners who have or had authorised access to an organisation's network, system, or data and intentionally misused that access to negatively affect the confidentiality, integrity or availability of the organisation's information or information system (Cappelli et al., 2012). Since social media is vulnerable, there is a high possibility of being attacked, which indicates the need for effective cybersecurity in organisations.

Cybersecurity of Organisation

The extensive use of social media by organisations requires cybersecurity to mitigate the consequences towards organisations. Cybersecurity protects networks, computers, and programs from unauthorised access and loss through attacks on the Internet (Das, 2017). Cybersecurity is the protection towards an organisation's data from attacks by internal or external actors. Social media exposes organisations to the problem of cybersecurity and also contributes to increasing the threats of cyberattacks (Ali et al., 2019). The cybersecurity threats in social media include social engineering attacks, lack of social media policy and scams {Formatting Citation}.

Social engineering refers to an attack on information security for accessing systems or networks (Syafitri et al., 2022). Social engineering attack on social media involves several steps, which are information gathering, examination of social networking media, tailored social engineering and sensitive insider information (Thakur et al., 2019). Social engineering is the exploitation of human fallibility and gullibility to distribute malware (Laudon, 2017). This kind of cybersecurity threat could harm social media. Organisations without social media policies or guidelines have endangered their organisations (Thakur et al., 2019). The most important things that must be addressed in a social media policy are: (1) the person who is allowed to represent on behalf of the organisation, (2) what they are allowed to say, (3) proper training for employees to manage the organisation's social media and (4) appointment of social media manager (Thakur et al., 2019).

Another cybersecurity threat in social media is scams. Cybercriminals often target social media such as Facebook and Twitter to conduct horrible cybercrimes (Thakur et al., 2019). Cybercriminals use various tactics to carry out scams on organisations' social media accounts, such as brand impersonation. Impersonation is the act of attempting to deceive someone by pretending he is another person (Gharawi & Badawy, 2021). Brand impersonation refers to a fake social media account of a particular organisation or brand in which irresponsible individuals or groups manage to deceive the public. Recently, there have been cases of impersonation involving The Star, where unsafe sites have pretended to be The Star and its online news portal through Facebook-sponsored ads in a targeted attack (The Star, 2022). Impersonation scams have become more prevalent in recent years, and most renowned Malaysian brands have issued statements to make customers aware of such scams (Ping, 2022).

Other threats of social media include hacking, malware and spam. Hacking means gaining unauthorised access to the organisations' social media accounts (Rudman, 2011). Social

media sites such as Facebook, Twitter, LinkedIn, Pinterest, and Tumblr offer a worthy environment for hackers (Laudon, 2017). Malware is an exploit designed to take advantage of software vulnerabilities in a computer's operating system, web browser, applications, or other software components (Laudon, 2017). It includes various threats such as viruses, worms, Trojan horses, ransomware, and bots. Meanwhile, spam refers to receiving unwelcome messages and links through social media and using social media accounts to spam (Joseph, 2012). Those are several forms of cyberattacks in which social media is vulnerable to being attacked by cybercriminals or cyber crooks.

Due to these cybersecurity threats in social media, cybersecurity efforts must come into action to mitigate the consequences that could impact organisational reputation risk.

Methodology and Conceptual Framework

The methodology of this conceptual paper examines the organisation's reputation risk with regards to social media usage, mediated by the organisation's cybersecurity using the analysis of the existing literatures. The propositions of this study is developed to analyse the relationship between social media usage, organisation's cybersecurity, and organisation's reputation risk. Based on the above discussion, the following propositions were formulated:

Proposition 1: Social media usage may impact an organisation's reputation risk.

Proposition 2: Social media usage may impact an organisation's cybersecurity.

Proposition 3: Cybersecurity of an organisation may impact an organisation's reputation risk.

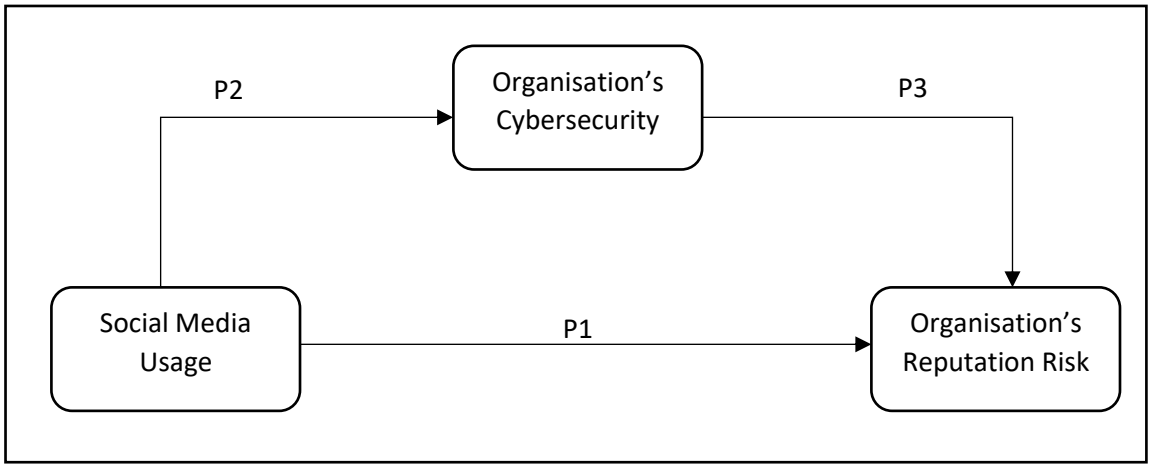

Figure 1 Proposed Framework

Conclusion, Limitations and Future Research

Organisations today prefer to exploit social media over traditional media. This is because there are various advantages to using social media. Still, at the same time, it is compulsory to identify the social media risks, take precautionary steps and be prudent while using social media. Building a reputation takes a long time, but reputation can destroy only overnight due to small things that significantly impact the organisation. Therefore, organisations need to take proactive measures to address risks. It is undeniable that organisations are unable to control social media in total; hence, organisations must take precautionary measures to ensure that reputational risks can be minimised.

Without a strategy, simply posting a message on social media can do more harm than good (Fullerton, 2011). For example, posting content stimulates reaction, generating unexpected results and network effects that can incur unexpected costs and outcomes for the

organisation, unlike what was initially planned. However, many organisations are unwilling or unable to develop strategies and allocate resources to engage effectively with social media (Kietzmann et al., 2011).

Social media usage has various risks, requiring cybersecurity to protect from being invaded by irresponsible parties. Cybersecurity threats in social media include social engineering attacks, lack of social media policy, and scams that could harm organisations. Social media has forced organisations to handle reputation risks that will negatively impact goodwill of the organisations (Mittal, 2015). Cybersecurity is important in mitigating organisations' social media risks and cybersecurity threats.

This paper identified social media usage in organisations, exposing them to various social media risks such as content, human, and technical risks. Using social media leads to cybersecurity threats that could affect an organisation's reputation risk. This paper figured out the linkage where social media exposed organisations to cybersecurity threats which eventually could damage an organisation's reputation.

This conceptual paper addressed a few limitations. First, the discussion is based on the literature review from past studies. The propositions, framework, and variables are formed based on the gaps identified regarding the cybersecurity organisation and the organisation's reputation risks from the earlier studies. Second, this paper only explains the variables and their relationship. The predictions of effects are based on the existing literature. There is still a lack of studies to show how social media, an organisation's cybersecurity and reputation risk relate to each other. Based on the limitations of the study, it is suggested that future studies could explore cybersecurity efforts with regard to social media usage and an organisation's reputation risks. Empirical research might be needed to determine how these constructs link to each other.

Acknowledgement

Authors acknowledge the Ministry of Higher Education (MOHE) for funding under the Fundamental Research Grant Scheme (FRGS) (FRGS/1/2021/SS01/UITM/02/9) with RMC File No. 600-RMC/FRGS 5/3 (050/2021).

References

Aguenza, B. B., Al-Kassem, A. H., & Som, A. P. M. (2012). Social Media and Productivity in the Workplace: Challenges and Constraints. *Interdisciplinary Journal of Research in Business*, *2*(2), 22–26. http://www.idjrb.com/articlepdf/article223.pdf

Ali, M. L., Thakur, K., & Atobatele, B. (2019). Challenges of cyber security and the emerging trends. *BSCI 2019 - Proceedings of the 2019 ACM International Symposium on Blockchain and Secure Critical Infrastructure, Co-Located with AsiaCCS 2019*, 107–111. https://doi.org/10.1145/3327960.3332393

Aula, P. (2010). Social media, reputation risk and ambient publicity management. *Strategy and Leadership*, *38*(6), 43–49. https://doi.org/10.1108/10878571011088069

Aula, P., & Mantere, S. (2013). Making and breaking sense: an inquiry into the reputation change. *Journal of Organizational Change Management*, *26*, 340–352. https://doi.org/10.1108/09534811311328380

Benthaus, J., Risius, M., & Beck, R. (2016). Social media management strategies for organizational impression management and their effect on public perception. *Journal of Strategic Information Systems*, *25*(2), 127–139. https://doi.org/10.1016/j.jsis.2015.12.001

Cappelli, D., Moore, A., & Trzeciak, R. (2012). *The CERT Guide to Insider Threars*. Pearson Education, Inc.

Cho, C.-C., & Wu, C.-H. (2014). Role of auditor in agency conflict and corporate governance. In *Chinese Management Studies* (Vol. 8, Issue 3). https://doi.org/10.1108/CMS-09-2012-0126

Choi, Y., & Thoeni, A. (2016). Social media: is this the new organizational stepchild? *European Business Review*, *28*(1), 21–38. https://doi.org/10.1108/EBR-05-2015-0048

Cotriss, D. (2022). *Small Business Guide to Social Media*. Business News Daily. https://www.businessnewsdaily.com/7832-social-media-for-business.html

Das, R. (2017). Cyber Security for Social Networking Sites: Issues, Challenges and Solutions. *International Journal for Research in Applied Science and Engineering Technology*, *5*(IV), 833–838. https://doi.org/10.22214/ijraset.2017.4153

Daud, S. H., & Othman, K. (2019). Awareness of social business in social media in malaysia. *Management and Accounting Review*, *18*(1), 139–166. https://doi.org/10.24191/mar.v18i1.832

De Lange, A. H., De Witte, H., & Notelaers, G. (2008). Should I stay or should I go? Examining longitudinal relations among job resources and work engagement for stayers versus movers. *Work and Stress*, *22*(3), 201–223. https://doi.org/10.1080/02678370802390132

DeLoach, J. (2018). *10 Ways Social Media Impacts Your Risk Profile | Corporate Compliance Insights*. Coroporate Compliance Insights. https://www.corporatecomplianceinsights.com/social-business-means-risk-profile/

Deloitte. (2014). *2014 global survey on reputation risk Reputation @ Risk " We don ' t see management as and end date .". October*.

Fullerton, R. (2011). *the Impact of Social Media on Marketing Strategy*. *February*.

Gharawi, M. A., & Badawy, A. (2021). *Social Media Impersonation in the Virtual World*. *4*(1). https://doi.org/10.46722/hkmh.4.1.21c

Gibbs, T. (2020). Seeking economic cyber security: a Middle Eastern example. *Journal of Money Laundering Control*, *23*(2), 493–507. https://doi.org/10.1108/JMLC-09-2019-0076

Gruber, D. A., Smerek, R. E., Thomas-hunt, M. C., & James, E. H. (2014). The real-time power of Twitter: Crisis management and leadership in an age of social media. *Business Horizons*. https://doi.org/10.1016/j.bushor.2014.10.006

Hausmann, V., & Williams, S. P. (2014). *Categorising Social Media Business Risks*. *4*.

Heil, D. (2018). Reputation Risk. *The International Encyclopedia of Strategic Communication*, *August 2018*, 1–6. https://doi.org/10.1002/9781119010722.iesc0150

Horn, I. S., Taros, T., Dirkes, S., Hüer, L., Rose, M., Tietmeyer, R., & Constantinides, E. (2015). Business reputation and social media: A primer on threats and responses. *Journal of Direct, Data and Digital Marketing Practice*, *16*(3), 193–208. https://doi.org/10.1057/dddmp.2015.1

Hovener, A. M., & Risk, R. (2015). *Corporate Reputational Risk Management : The Power of Social Media*. 1–15. http://essay.utwente.nl/68528/

Joseph, R. C. (2012). E-Government Meets Social Media: Realities and Risks. *IT Professional*, *14*(1).

Kaplan, A. M., & Haenlein, M. (2010). *Users of the world , unite ! The challenges and opportunities of Social Media*. https://doi.org/10.1016/j.bushor.2009.09.003

Kapoor, K. K., Tamilmani, K., Rana, N. P., Patil, P., Dwivedi, Y. K., & Nerur, S. (2018). Advances

in Social Media Research: Past, Present and Future. *Information Systems Frontiers*, *20*(3), 531–558. https://doi.org/10.1007/s10796-017-9810-y

Kaul, A., Chaudhri, V., Cherian, D., Freberg, K., Mishra, S., Kumar, R., Pridmore, J., Lee, S. Y., Rana, N., Majmudar, U., & Carroll, C. E. (2015). Social Media: The New Mantra for Managing Reputation. *Vikalpa*, *40*(4), 455–491. https://doi.org/10.1177/0256090915618029

Kietzmann, J. H., Hermkens, K., McCarthy, I. P., & Silvestre, B. S. (2011). Social media? Get serious! Understanding the functional building blocks of social media. *Business Horizons*, *54*(3), 241–251. https://doi.org/10.1016/j.bushor.2011.01.005

Lange, D., & Lee, P. M. (2011). Organizational Reputation: A Review. *Journal of Management*, *37*(1). https://doi.org/10.1177/0149206310390963

Laudon, K. C. (2017). *E-commerce 2017: business, technology, society*.

Majchrzak, A., Faraj, S., Kane, G. C., & Azad, B. (2013). The contradictory influence of social media affordances on online communal knowledge sharing. *Journal of Computer-Mediated Communication*, *19*(1), 38–55. https://doi.org/10.1111/jcc4.12030

McCorkindale, T., & Distaso, M. (2013). The Power of Social Media and Its Influence on Corporate Reputation. *The Handbook of Communication and Corporate Reputation*, 497–512. https://books.google.com/books?id=1QfiKkvH4jIC&pgis=1

Mittal, S. (2015). Reputational Risk, Main Risk Associated with Online Social Media. *IJCC*, *34*(2).

Muller, J. (2021). • *Malaysia: company presence on social media by sector 2017 | Statista*. Statista. https://www.statista.com/statistics/1019862/malaysia-company-presence-on-social-media-by-sector/

Olanrewaju, A. T., Hossain, M. A., Whiteside, N., & Mercieca, P. (2020). Social media and entrepreneurship research : A literature review. *International Journal of Information Management*, *50*, 90–110. https://doi.org/10.1016/j.ijinfomgt.2019.05.011

Parveen, F., Jaafar, N. I., & Ainin, S. (2015). Social media usage and organizational performance: Reflections of Malaysian social media managers. *Telematics and Informatics*, *32*(1), 67–78. https://doi.org/10.1016/j.tele.2014.03.001

Perera, S., Jin, X., Maurushat, A., & Opoku, D. G. J. (2022). Factors Affecting Reputational Damage to Organisations Due to Cyberattacks. *Informatics*, *9*(1), 1–24. https://doi.org/10.3390/informatics9010028

Picazo-Vela, S., Gutiérrez-Martínez, I., & Luna-Reyes, L. F. (2012). Understanding risks, benefits, and strategic alternatives of social media applications in the public sector. *Government Information Quarterly*, *29*(4), 504–511. https://doi.org/10.1016/J.GIQ.2012.07.002

Pienta, D., Tams, S., & Thatcher, J. B. (2020). Can trust be trusted in cybersecurity? *Proceedings of the Annual Hawaii International Conference on System Sciences*, *2020-Janua*, 4264–4273. https://doi.org/10.24251/hicss.2020.522

Ping, O. L. (2022). *Shopee Malaysia warns public as more victims fall prey to employment scams*. Marketing Interactive. https://www.marketing-interactive.com/shopee-malaysia-warns-public-as-more-victims-fall-prey-to-employment-scams

Pretty, D. (2018). Reputation risk in the cyber age: The impact on shareholder value. *Aon & Pentland Analytics*.

Reuter, C., Ludwig, T., Friberg, T., Pratzler-Wanczura, S., & Gizikis, A. (2016). Social Media and Emergency Services? *International Journal of Information Systems for Crisis Response and Management*, *7*(2), 36–58. https://doi.org/10.4018/ijiscram.2015040103

Roshan, M., Warren, M., & Carr, R. (2016). Understanding the use of social media by

organisations for crisis communication. *Computers in Human Behavior*, *63*, 350–361. https://doi.org/10.1016/j.chb.2016.05.016

Rudman, R. (2011). USING CONTROL FRAMEWORKS TO MAP RISKS IN WEB 2.0 APPLICATIONS. *Accounting and Management Information Systems*, *10*(4), 495–515.

Sivertzen, A. M., Nilsen, E. R., & Olafsen, A. H. (2013). Employer branding: Employer attractiveness and the use of social media. *Journal of Product and Brand Management*, *22*(7), 473–483. https://doi.org/10.1108/JPBM-09-2013-0393

Soprano, A., Crielaard, B., Piacenza, F., & Ruspantini, D. (2010). *Measuring operational and reputational risk: A practitioner's approach* (Vol. 562). John Wiley & Sons.

Spanier, G. (2015). Reputation Risk in the social media age. *Raconteur*, 1–30. http://raconteur.net/business/reputational-risk-in-the-social-media-age

Syafitri, W., Shukur, Z., Mokhtar, U. A., Sulaiman, R., & Ibrahim, M. A. (2022). Social Engineering Attacks Prevention: A Systematic Literature Review. *IEEE Access*, *10*, 39325–39343. https://doi.org/10.1109/ACCESS.2022.3162594

Tajudeen, F. P., Jaafar, N. I., & Ainin, S. (2018). Understanding the impact of social media usage among organizations. *Information and Management*, *55*(3), 308–321. https://doi.org/10.1016/j.im.2017.08.004

Thakur, K., Hayajneh, T., & Tseng, J. (2019). Cyber Security in Social Media: Challenges and the Way Forward. *IT Professional*, *21*(2), 41–49. https://doi.org/10.1109/MITP.2018.2881373

The Star. (2022). *Scam alert: Fake sites target The Star with shady Facebook ads | The Star*. The Star. https://www.thestar.com.my/news/nation/2022/04/11/scam-alert-fake-sites-target-the-star-with-shady-facebook-ads

Ursillo, S., & Arnold, C. (2019). *Cybersecurity Is Critical for all Organizations – Large and Small | IFAC*. International Federation of Accountants. https://www.ifac.org/knowledge-gateway/preparing-future-ready-professionals/discussion/cybersecurity-critical-all-organizations-large-and-small

Van Osch, W., & Coursaris, C. K. (2013). Organizational social media: A comprehensive framework and research agenda. *Proceedings of the Annual Hawaii International Conference on System Sciences*, *December*, 700–707. https://doi.org/10.1109/HICSS.2013.439

Wilson, J. (2009). Social networking: The business case. *Engineering and Technology*, *4*(10), 54–56. https://doi.org/10.1049/et.2009.1010

Xia, L. (2013). *Effects of Companies ' Responses to Consumer Criticism in Social Media*. *17*(4), 73–99. https://doi.org/10.2753/JEC1086-4415170403

Zerfass, A., Fink, S., & Linke, A. (2016). Social Media Governance: Regulatory Frameworks As Drivers of Success in Online Communications. *14th International Public Relations Research Conference*.