Risks, Privacy and Responsibility of Social Media use in the Workplace: A Review

Bert Noble[a], Samantha Collen[a], Craig Overboe[a] and Akalanka Mailewa[b]

[a]Department of Information Systems, St. Cloud State University, St. Cloud, MN, United States

[b]Department of Computer Science and Information Technology, St. Cloud State University, St. Cloud, MN, United States

Abstract

Technology advances keep pushing the digitalization of processes in the workplace, leading to an increased use of internet and social media platforms. Little has been done to define and implement the risks and implement policies to protect against these risks. This review looks at the risks associated with the use of social media in the workplace. Looking at literature from the past decade, the risks are defined and discussed, and the two main topics that can mitigate those risks are discussed more thoroughly: 1) privacy policies, regulations, and strategic plans, and 2) the importance of regular employee security, education, training, and awareness (SETA) programs. This review adds to existing literature by creating a conceptual overview of all risks found in earlier research and by defining future areas of research for further analysis.

Keywords: Social Media, Workplace, Privacy, Responsibility, Risks, Digitalization

Introduction

The internet and use of social media platforms is growing exponentially, and the volume, variety, and velocity of data is making it difficult for existing systems to prevent new attacks and data breaches (Huerta & Jensen, 2017; Basil et. al., 2022). Due to an increase in the number of data breaches and the intensity of damage caused to an organization by a breach, it is vital that individual employees, businesses, and governments address digital privacy and responsible issues (Huerta & Jensen, 2017; Warner & Wäger, 2019; Basil et. al., 2022). This exploration of research provides an overview of privacy and responsibility issues related to social media use in the workplace.

As the world continues to undergo the digital transformation, the popularity and commoditization of the internet as a form of communication and retail increase the pressure on businesses to transform and innovate their business models (BM) and business strategies to keep up with the new markets and stimuli (Caputo et al., 2021; Bouwman et al., 2019). It has been shown that contributing resources to digitalization, particularly social media networks, increases company performance (Ribeiro-Navarrete et al., 2021). Social media, also known as social media platforms, or social networking sites (SNS) (Hajli & Lin, 2016) are changing the way businesses advertise products, collect data, and interact with customers. Social media is the most valuable and critical form of digitalization (Prodanova & Van Looy, 2019).

According to a 2021 survey performed by the Pew Research Center, 72% of Americans say they use social media platforms (Auxier & Anderson, 2021). The breakdown of social media use by age group can be seen in Table 1. The popularity and commoditization of social media and the positive impact it has on business productivity and profitability makes social media one of the most important tools for improved communication between individuals, between customers and companies, and for business to business (B2B) communication (Prodanova & Van Looy, 2019). Prodanova and Van Looy (2019) found that an investment in social media, maintaining updated social media content, and regular technology staff trainings lead to an increase in business financial performance.

Due to the vast quantity of personal information shared on social media, information sharing has become a crucial issue of privacy and security debate (Hajli & Lin, 2016). Some critical ethical and privacy concerns that arise from social media data collection are the use of personal information by businesses for organizational profit and gain (Hajli & Lin, 2016), data use by the social media site itself, and data

Table 1: Percent of Social Media Users by Age Group

Age Group of Users	Percentage of Social Media Users
18 - 29	84%
30 - 49	81%
50 - 64	73%
65 and older	45%

exposed knowingly or unknowingly from users' signing up for scams or online applications that require access to their social profile, contact list(s), or access to their digital devices (Hajli & Lin, 2016). Social media site users need better control over their own data and should have more control over the information they share. Social media sites are giving users more control of their own privacy, by designing privacy settings, and implementing privacy policies (Hajli & Lin, 2016).

Research methodology

For this literature review, the authors compiled a list of existing research with the goal of identifying gaps and possibilities for future research within the domain of social media, privacy, and responsibility, focusing on the workplace. This review starts with the formulation of the main research question:

RQ1: What are the challenges and associated risks of social media use in the workplace?

To answer this question the authors created a mind map of all the risks that were prevalent in the existing research. The review also indicates in what areas additional research is possible. Based in the outcomes of RQ1, the authors focused on two main areas within the identified risks to formulate two additional research questions:

RQ2: What are the regulatory frameworks touching the issues of social media use in the workplace, and what are the recent advances in the governance realm?

RQ3: Who is tasked with ensuring responsible social media use in the workplace and what are the recent advances in the awareness realm?

Within RQ2 and RQ3, the authors identified existing frameworks and research, mainly linked to the privacy risks, and focused on the recent advances and possible future research.

Risk of social media use in the workplace

The digitalization of businesses has increased the use of social media up to a point where one might ask if the risks involved in the use still out way the benefits. Figure 1 shows a broad overview of the risks that were identified by this research. This review paper describes how the different risks influence the decision-making process for both the business itself and for its employees. It uses existing research to summarize the various risks of social media use and focuses on the major problems: privacy, responsibility, and the lack of governance.

Figure 1: Social Media Risks – Employer and Employee Point of View

Social Media Risk Management

Deloitte stated in 2012 that the financial risk that potentially comes from social media use is a major concern for company leadership (Demek et al., 2018; Soens & Claeys, 2021). Nevertheless, surveys have shown that only a minority of senior managers know if their company performs a formal risk assessment of social media

use (= proactive risk management approach) (Demek et al., 2018). Research shows that governance of social media risks is generally done through the creation of policies (Demek et al., 2018; Soens & Claeys, 2021; Yokoyama, 2016). Many companies have a form of social media policy that has been created without a formal risk management process (= reactive risk management approach) (Demek et al., 2018). In their 2018 research paper, Demek et al. use the existing COSO enterprise risk management – integrated framework (ERM-IF) to develop a tailored social media risk management model (SM-RMM) to determine the type of approach organizations use to manage the social media risk (Demek et al., 2018).

The policies that organizations use to mitigate the risk can either be restrictive or incentive, the first category trying to avoid the risk, the latter category trying to encourage the individuals to a social media use beneficial to the organization (Soens & Claeys, 2021). A New Zealand master thesis on the perceived risks of the use of personal devices by student nurses during internships reinforces the idea that formal restrictive policies are necessary, but that especially the younger generation needs incentives to put aside this useful tool. Research by Yokoyama (2016) also shows that the use of smartphones and social media in the workplace has a potential risk of data leakage. Not only employers have to engage in social media risk management, so do employees. Because of their ability to quickly adopt new technologies, young people especially are more susceptible to becoming social media dependent (Jeri-Yabar et al., 2018). The study done by Jeri-Yabar et al. (2018) shows that there is a direct correlation between the time spent on social media and the existence of depressive symptoms. In the same study they also show that people with depression symptoms prefer Twitter over the other SMP (Jeri- Yabar et al., 2018).

Potential for future research: the additional risks introduced to the work environment by allowing to BYOD, the impact or value of work agreements to include an online aspect.

Figure 2: Social media risk management – keywords

Social media use and decision making

Social media use usually entails the sharing of content, information, and opinions. The availability of this type of information encourages people to either investigate more into certain topics or will help them in their decision-making (Kapoor et al., 2017; Yokoyama, 2016). Although there have been many papers that have researched the behavioral side of the use of social media, it is important to also look at the inherent risks. Unfortunately, the risk of social media use has been in the shadow for too long and merits additional attention and research (Kapoor et al., 2017; Demek et al., 2018; Yokoyama, 2016).

Figure 3: Social media use and decision making – keywords

One of the major fields that can benefit from the explosion of social media use is human resources, through the process of cybervetting (Melton et al., 2020). However, Yokoyama (2016) advocates that this comes with an increased responsibility. When using social networks' sites to gain information on the private life of potential employees, organizations can reduce the cost of the recruitment process through direct access to work history, potential disqualifying information, or direct contact with social connections from the applicant (Yokoyama, 2016; Krings et al., 2021; Melton et al., 2020). Fake profiles, incomplete and incorrect information, and the tendency of people to act and post differently depending on the context remains a concern (Yokoyama, 2016). Making it important that human resources' decisions aren't solely based on information from SNS (Yokoyama, 2016; Melton et al., 2020). An additional factor to limit the use of social media posts in human resources processes, is the fact that there is a difference between generations in the quality and number of posts (Krings et al., 2021). In the same way, recruiters need to be aware that on professional SMPs like LinkedIn, which are the one place where individuals will showcase their capabilities

and skills, with the sole purpose of creating an attractive profile for potential employers, there are also differences between older and younger generations regarding the posting of skills, qualifications, and references (Krings et al., 2021). Some of these differences are directly related to the fact that younger people grew up with SNS, while older people had to learn to use SNS (Krings et al., 2021). Yokoyama (2016) states in his research that it is vital that an organization is transparent about the use of social media in its decision-making processes. This is certainly the case if employers use the lack of online information as a reason for not trusting a potential candidate (Melton et al., 2020). A study from Prost in 2007 shows that recruiters uncover negative information about potential employees in approximately 34% of the searches (Miller et al., 2010).

Potential for future research: transparency of employers in the use of social media in the hiring process, the influence of not having social media accounts on the current hiring and promotion processes.

Spying on employees through social media

The sheer amount of information that people share on social media makes it a valuable source of data for the (future) employers. The research in Yokoyama (2016) and Melton et al. (2020) shows that monitoring employees proves to provide the employer with information that can be used during the performance reviews with possible effects on employee's salary and or employment. This is especially true when dealing with internships and entry-level positions (Melton et al., 2020). The rise in #NSFW ('not safe for work: consensually shared sexual content) posts on more recent SMP like OnlyFans may become a reason for dismissal, even though it may not have a direct impact on performance (Morris, 2021). The fact that users post material that can be harmful in their real life or in their career, showcases the posting paradox (Melton et al., 2020). A major reason for cybervetting the personal social media posts of employees, is the possible reputational damage that can occur (Kapoor et al., 2017; Melton et al., 2020), although there may be some ethical issues when employers start using different standards based on gender or national culture (Melton et al., 2020). Not only data which is intentionally posted on social media contains valuable information. Through profile information mining activities, it is possible to discover information by aggregating and correlating data and metadata (Kapoor et al., 2017; Majmundar et al., 2019). This data aggregation could potentially lead to identity theft (Kapoor et al., 2017). A negative effect that is reinforced by the persistence of the data that is online: every piece of data that is posted online leaves the control of its owner and is almost impossible to delete entirely and everywhere (Zurbriggen et al., 2016). Within this category of risk, it is important to mention online social transparency, where employees, using the company's collaboration tools, provide information to their colleagues and the employer about their own activity status (Alsaedi et al., 2021). Adverse effects of this form of transparency include peer pressure to be online at all times, the availability of an overload of useless information about colleagues and teams, and judgement based on their status or updates (also known as social loafing) (Alsaedi et al., 2021).

Potential for future research: development of a program that teaches users to become savvy social media users, the effect of #NSFW posts on an individual's personal life, the accepted level of scrubbing your social media to pass cybervetting.

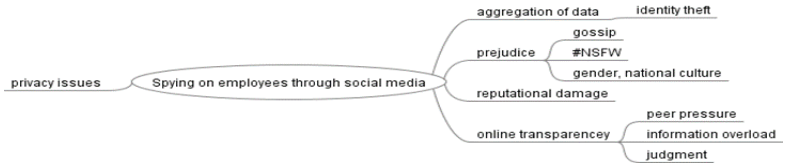

Figure 4: Spying on employees through social media – keywords

Victimization at work and its consequences

Cyberbullying is different from traditional bullying in the fact that one committing the bullying has the possibility to stay anonymous. All other elements like aggression, power imbalance and repetitive character are the same (Oksanen et al., 2020). Cyberbullying victimization, including damaging gossip may have serious cumulative consequences for the victim and the employer, including psychological stress leading to depression and sick leave, and work exhaustion leading to decreased productivity and additional burden for coworkers (Oksanen et al., 2020; Cowan & Horan, 2017; Jeri-Yabar et al., 2018). Research shows that the effects are correlating with the level of intensity of one's digital social life and the level one's personality is defined by its virtual social identity (Oksanen et al., 2020). Online versions of sexist and hate speech, or

online harassment of minorities, show that the boundaries of the workplace have expanded into our social media profiles (Morris, 2021). The anonymity of social media also lead to an increased level of radicalization, especially on Twitter (Lara-Cabrera et al., 2019).

Potential for future research: all aspects of cyberbullying, all aspects of cyberstalking, the link between online victimization and radicalization.

Figure 5: Victimization at work and its consequences – keywords

Privacy Policies, Regulations, and Strategic Plans

Although social and business digital process transformation has been occurring for decades, there are many unanswered questions of responsibility and privacy concerns. There are few regulations in place to mitigate those concerns. Among these policies is the General Data Protection Regulation (GDPR) (Council of the European Union, 2016). This information privacy governance policy outlines protection measures and users' rights to data privacy. The policy protects citizens from the European Union by providing governance and guidelines for organizations, outlining how to properly collect, store, and process customer data. The GDPR gives customers control of their data (Zaman & Hassani, 2020). Research by Zaman and Hassani (2020) outlined three measures for verifying privacy compliance standards (data cleansing compliance, subject permissions/rights data mining compliance, and scheme to compare data security compliance processes). These compliance measures help businesses monitor, maintain, and improve GDPR compliance. Their research proposed two tools to help businesses record and compare measurable privacy and compliant outcomes. Once a business is within compliance, it is vital that it maintains compliancy by continually monitoring and adjusting compliancy deviations (Zaman & Hassani, 2020).

The healthcare industry and financial institutions are bodies governed by the most legislation. In the past decade, healthcare has transitioned to digital processes – collecting, transmitting, and storing patients' data online rather than on paper. The Federal Health Information Technology Strategic Plan (HITECH) (2009) and financial incentives have greatly encouraged and increased the number of electronic health records (EHRs). This move to EHRs has created concerns about the unauthorized release of personal healthcare data (Basil, et. al., 2022). In addition to financial incentives, the law also introduced penalties for healthcare providers not in compliance with the 1996 Health Insurance Portability and Accountability Act (HIPAA). HIPAA outlines how healthcare and third-party insurance companies share data and maintain data confidentiality and data integrity. Even with these policies in place, every year the healthcare industry loses $6.5 million due to data breaches and healthcare information privacy compromises (Basil, et. al., 2022). In a digital world, where healthcare data is shared and stored online, there is a need for better and more strategic information security measures (Basil, et. al., 2022).

Like the healthcare industry, the financial and accounting industry have moved to online banking and financial processes. The shift of accounting from paper to digital data storage has shifted the industries' information security concerns and mitigation controls from the physical to the digital. Legislation such as the Gramm-Leach-Bliley Data Protection Act (GLBA) (1999), and the Sarbanes-Oxley Act (SOX) have guidelines for information privacy specific to Europe and U.S. accountants respectively. However, the increase in data storage and the variety of stored data formats (big data) has increased the risk of data breaches (Huerta & Jensen, 2017). The popularity and incentives to mine data for sale has increased risks to businesses and customers' privacy. According to Huerta and Jensen (2017), the biggest risk to a business due to a data breach and poor information security is the loss of customers' confidence. This can affect businesses longevity and performance for years. Privacy standards are continually evolving to address the new issues from big data. Researchers and accountants should be open to digital change, and educators should prepare accounting students with developing cybersecurity, auditing, and analytical skills (Huerta & Jensen, 2017).

An established privacy policy that focuses on educational institutes and students before they reach the labor force is the Family Educational Rights and Privacy Act (FERPA). The act was put into law in 1974, to protect the confidentiality of students' personal identifiable information. With the addition of technology in

traditional education and the use of collaborative tools for online remote learning there is the risk of exposing students' personal information. FERPA outlines violations and strategies to avoid privacy issues (Sevignani, 2013; Schrameyer et al., 2016).

According to Sevignsni (2013), the concept of privacy on the internet has been commodified, meaning it is exchanged on the market. Although policies should be fair for all, powerful economic players are able to effect and manipulate policies and politics to support their personal interests and those of their stakeholders. Sevignsni (2013) determined that the practice of using data collected from social networking sites conflicts with users' need for privacy. The public privacy process is not capable of solving the privacy problem. Criteria and strategic solutions, along with the legal, self-regulatory, and technical issues are proposed. The Electronic Privacy Information Centre (EPIC) (Europe v. Facebook) is an example of a self-regulatory civil initiative that should be recognized (Sevignsni, 2013).

Sánchez et. al. (2012) cited Erving Goffman's 1959 book stating that humans control others' impressions of them by establishing and maintaining segregated identities (personas or actors) on social media platforms. Sánchez et. al. (2012) stated that Goffman's view that professionalism in the workplace requires that users' employee persona and private persona remain segregated is even more relevant today due to technology and social media. Privacy laws in the United States are based on this separation of physical and social entities. An example of crossing these privacy boundaries can be seen in the U.S. Supreme Court case City of Ontario v. Quon. Officer Quon's employer accessed his personal text messages sent from his employer-owned device. The court admitted it was unsure how the means of rapidly changing digital communication would affect future employers' privacy expectations. The U.S. is not the only nation unsure of digital privacy legislature, stating that the world is having problems finding and securing data privacy in the digital age. Examples include the debate of the "right to be forgotten" proposed in Europe to address privacy issues with long-term data storage, and the Canadian supreme court stating it would postpone privacy issue cases related to technology, until they can analyze and organize digital privacy issues into a report (Sánchez et. al., 2012). Sánchez et al. (2012) surveyed working millennials about privacy and social media use in the workplace. He found that millennials wanted a separation of personal and work personas, but they recognized that the societal importance of social media made it so they could not withdraw themselves to protect their privacy. Other measures need to be considered. Technology, digitalization, and social media need to establish regulations, norms, and legal controls to prevent suppression and personal privacy breaches (Sánchez et. al., 2012).

According to Rice and Sussan (2016), digital privacy must be understood by business management to protect personal privacy and maintain the trust of business stakeholders. Business information security and governance controls give context to understanding digital privacy. According to Rice and Sussan (2016), there are three factors that form the trust between a business and its customers, 'what', 'why', 'how'. These factors are displayed in Figure 1: Trust factors between business and customers. Business and regulations define 'what' data must be protected. Financial institutes (i.e. banks), health institutions (ie. doctor's office), and accounting firms (ie. tax office) are examples of businesses that must follow strict data privacy regulations. Regulations in place include the Gramm-Leach-Bliley Data Protection Act (GLBA) (1999), USA Patriot Act (section 314), Sarbanes-Oxley Act (SOX) (2002), Payment Card Industry (PCI) Security Standards, and other state and local laws (Rice & Sussan, 2016). The 'why' is for digital privacy to protect digital assets. The 'how' is defined by the information security policies and practices of the business. This includes methods of storage, transmitting, and access control. Both physical and digital measures must be considered. Customers' data privacy is at the center of debate for businesses, researchers, and government leaders (Rice & Sussan, 2016).

There are many unanswered privacy and ethical issues that arise from social media network use (Haiji, et. al., 2016). Even more questions arise when it comes to businesses' use of social media in terms of their customers, employees, the organization, and its stakeholders.

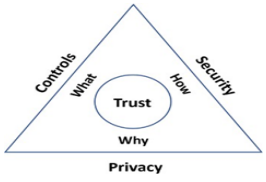

Figure 6: Trust Factors between Business and Customers

Potential for future research: responsibility in case of a data breach (business, user, SMS), necessity of privacy policies and governance oversite (government, third-party agency, SMN, business, user)

Responsibility for privacy issues in the workplace

When it comes to the privacy issues in the workplace, the question "who is responsible" comes up quite often. Users may suggest privacy is the responsibility of the Cybersecurity experts using security tools to protect the environment. Management might insist it is the responsibility of the user, while the Cybersecurity professionals might suggest it is the responsibility of both management and the end user. So, who is correct? The answer is that it is everyone's responsibility. However, just to say "it is everyone's responsibility" is not enough, to evaluate responsibility, we must also evaluate obstacles to achieving privacy in the workplace for both internal and external customers. When it comes to user responsibility, there needs to be sufficient motivation on their part. Upper management, of course, can order employees to take training. However, a better way to motivate employees is to create an environment where security is everyone's top priority. Therefore, the individuals responsible for creating the curriculum for the Security Education Training and Awareness (SETA) program must look at innovative engaging approaches to ensure their program is not just one-size-fits-all. Recent advances and research in Cybersecurity training have found many innovative approaches to create more salient content that users will internalize in a greater capacity. A bottom-up approach is often encouraged by ensuring employees are educated on up-to-date security best practices. If every employee in the security chain does their part, it will ensure the whole organization is safe, after all, a chain is only as strong as its weakest link (Lykou et al., 2018).

The organization may have the latest cybersecurity technology, but human factors must be considered, including awareness and skill training programs (Carlton & Levy, 2015). Price Waterhouse Coopers research indicates that between 72% and 95% of sources of cyber threats come from ignorant information cybersecurity practices among former and current employees. (D'Arcy & Hovav, 2007; IBM Global Technology Services, 2014; Landress et al., 2017). Cybersecurity awareness is vital to the organization because it specifies the level at which the company is ready for cyber-attacks and how well the employees understand cybersecurity threats. However, some organizations are overly dependent on SETA models, making this the core of their cybersecurity culture. The primary concern is an over-reliance on cybersecurity awareness training programs, some companies think these are the remedy for cybersecurity breaches. This over-dependency and high expectations from upper management do not promote a healthy security climate. (Proctor, 2016). For an organization to be effective in their awareness, employees should be subjected to cybersecurity threats while learning the cause and effects of the threats and learn to counter them (Ansari, 2022). This creates a shared sense of responsibility among employees while simultaneously reducing the burden on company cybersecurity professionals.

Recent advances in creating an effective SETA program

In 2010, The National Institute of Standards and Technology (NIST), created the National Initiative for Cybersecurity Education (NICE) framework, a model developed by industry experts and academia for cybersecurity awareness, training, and to develop a stronger cybersecurity aware workforce. The NICE framework gives broad guidance to develop curriculum, but because of the lack of domain experts, companies face difficulties using it. To overcome this challenge, Amazon created the viCyber cloud-based system that uses AI and visual mappings, this intelligent system capable of rapid training development of cybersecurity curriculum (Wang et al., n.d.).

Dash and Ansari (2022) proposed the Technology Acceptance Model (TAM). This research is based on previous work of the Technology Adoption Model, a model that recreated an influential role in information management (Davis, 1989). However, TAM introduced the new variable “behavioral intention” indicating that information security awareness training execution are successful interventions for at-risk employee behavior. The study examined the effectiveness of AI-based security awareness training programs on employee behavior and helped analyze SETA workplace training, encouraging behavioral transformations by incorporating user exposure to cybersecurity topics to reduce data breaches (Dash & Ansari, 2022). According to Khan et al. (2023), Protection Motivation Theory (PMT) is a popular cybersecurity behavioral research theory and was used to understand user behavioral change after cybersecurity training implementation (Hutchinson & Ophoff, 2020; Boehmer et al., 2015; Johnston & Warkentin, 2010). Their evaluation used the three levels of Kirkpatrick's evaluation model: behavior, learning, and reaction. The

core of the PMT theory is that individuals enact certain behaviors to avert threats. The decision to carry out these actions is governed by threat and coping appraisal, the two core components of PMT (Rogers, 1983) which play a key role in behavior change. The Components of PMT map well to security concepts and the theory is favored by security researchers (Sommestad et al., 2015).

Goode et al. (2018) conducted an organizational cybersecurity program expert assessment and developed cybersecurity countermeasures awareness vignettes for measurements. The authors theorized that while training initiatives existed, studies of empirical research that focused on what should be encompassed in security education, training, and awareness (SETA) programs were limited. In their study, they interviewed subject-matter experts (SMEs) to validate the key typical & socio-technical SETA program topics needed: cybersecurity countermeasures awareness (CCA) employee measurement criteria, policy awareness weights, SETA, & monitoring of the CCA categories, and SETA program content with integrated CCA vignette-based assessments. They used a Delphi methodology to gather cybersecurity topic feedback from 21 SMEs for organizational SETA programs, validation of SETA training content, and to develop a vignette-based measure of CCA. Results showed that the most important category was awareness of the organizational cybersecurity policy for the overall CCA measure at 41%, followed by SETA program content awareness at 34%, while monitoring awareness was 25%. (Pratama et al., 2023) offer that because authentication mechanisms such as passwords are the most prevalent cybersecurity measure employed today. Therefore, increasing user awareness of what makes a password strong should be a high priority for companies. Situated learning posits that effective learning occurs through connections made between authentic prior knowledge and often informal unintended contextual learning, compared to traditional learning using abstract and out-of-context experiences like lectures and books (Clancey, 1995; Northern Illinois University Center for Innovative Teaching and Learning, 2012). As such, users in situated learning settings are engaged in real-world activities that require them to apply knowledge and apply critical and problem-solving thinking. They put forward the idea of a dynamic password meter that changes in real-time as the user puts in each character while establishing their passwords would result in improved knowledge and, consequently, awareness. In their work, they conducted a survey experiment with 168 IT students from Indonesia and Saudi Arabia to see if different approaches in the form of educational infographics yielded different results in terms of user knowledge of password strength.

In their article "Managing Organizational Cyber Security–The Distinct Role of Internalized Responsibility" Faltermaier et al. (2023) believe that desirable user behavior is key to cybersecurity. However, they also suggested that “how to manage user behavior to support organizational cybersecurity effectively” comprehensive overview was missing. They based their analysis on twenty interviews with users and IT managers of a university in Europe to build upon current research to identify central cybersecurity management components. They contribute to understanding the relationships between user awareness and behavior, technology capabilities, organizational information technology, and “internalized responsibility” as it relates to cybersecurity in the organization (Faltermaier et al., 2023).

A different methodology comes from Sadaghiani-Tabrizi (n.d.) in the article “Revisiting Cybersecurity Awareness in the Midst of Disruptions". The author posits that awareness of cybersecurity threats taught as early as K-12 can help mitigate risks and create a more cyber-secure-aware future workforce. Partnering with IT to reform educational means will facilitate efficiency, drive innovation, and channel effective information exchange which surrounds Internet information access and retrieval processes (The Levin Institute, 2014). A qualitative case study narrative explored prospects for integrating cybersecurity education into elementary school curriculum through elementary school teachers’ interviews, IT experts, and parents to gain feedback about perceptions of cybersecurity knowledge and awareness. The focus was on facilitating content through collaboration among peers to advance digital communication-supported learning strategies for the implementation of cybersecurity in education, directing attention to leaders' clear vision for cybersecurity and skills to assess safety in protecting sensitive or private information (Sadaghiani-Tabrizi, n.d.).

Zafar et al. (2023) used an action research approach to work toward an effective SETA program. Their research related to self-regulation theory to create a new security education training and awareness (SETA) program that focused on password-sharing, phishing awareness, and unauthorized cloud service use threats. In regard to learning philosophy, the learning approach of self-regulation is different from learning involving traditional behaviorist approaches (Rumjaun & Narod, 2020). Self-regulation theory emerged from social cognitive theory and aids in learning that result in student’s self-generated behaviors and

cognitions (Schunk & Zimmerman, 2003), and action research was the ideal method for refining and validating the SETA program (Checkland & Holwell, 1998). Their findings indicated that the training effectively helped users identify or avoid cybersecurity environmental threats, therefore the new SETA program was more effective than the existing one.

Finally, Nwachukwu et al. (2023) asked the question "Do SETA Interventions Change Security Behavior?" In their literature review, they conducted SETA program interventions to study effects on user cybersecurity behavior. However, they posit that collective knowledge on how SETA influences behavior is lacking. Based on their review, they concluded that SETA interventions do have the potential to influence cybersecurity behavior. Successful intervention evidence from prior research was found, however, effective design method prescriptions regarding what specific design choices make the most effective training methods remains anecdotal. Their research has contributed to narrowing the SETA program gaps by proposing six tentative design recommendations for effective SETA interventions. Those recommendations include: 1) interactive participant engagement, 2) relevant context, 3) user-specific task/threat tailored training, 4) strong, concrete fear appeal messages, 5) regular training, and 6) skill development.

Conclusion

Technology advances keep pushing the digitalization of processes in the workplace, leading to an increased use of internet and social media platforms. Our research looked at the risks associated with the use of social media in the workplace through a literature review from the past decade. Research suggests that continued exploration and analysis of all issues, including but not limited to privacy, and the implementation of privacy policies surrounding the social media use in the workplace are necessary. There are ample opportunities for future research, including in our two focus areas, the governance of privacy risks and the creation of SETA programs.

References

Alsaedi, T., Sherief, N., Phalp, K., & Ali, R. (2021). Online social transparency in enterprise information systems: Arisk assessment method. *Information Technology and Management*, 23(2), 95–124. https://doi.org/10.1007/s10799-021-00347-3

Ansari, M. F. (2022). A quantitative study of risk scores andthe effectiveness of AI-based Cybersecurity AwarenessTraining Programs. *International Journal of Smart Sensor and Adhoc Network*., 1–8. https://doi.org/10.47893/ijssan.2022.1212

Auxier, B., & Anderson, M. (2021). Social Media Use in 2021. *Pew Research Center*. https://www.pewresearch.org/internet/2021/04/07/social-media-use-in-2021/

Basil, N. N., Ambe, S., Ekhator, C., & Fonkem, E. (2022). Health Records Database and Inherent Security Concerns: A Review of the Literature. *Curēus* (PaloAlto, CA), 14(10), e30168–e30168. https://doi.org/10.7759/cureus.30168

Boehmer, J., LaRose, R., Rifon, N., Alhabash, S., & Cotten, S. (2015). Determinants of online safety behaviour: Towards an intervention strategy for college students. *Behaviour & Information Technology*, 34(10), 1022– 1035. https://doi.org/10.1080/0144929x.2015.1028448

Bouwman, H., Nikou, S., & de Reuver, M. (2019). Digitalization, business models, and SMEs: How do business model innovation practices improve performance of digitalizing SMEs? *TelecommunicationsPolicy*, 43(9), 101828– https://doi.org/10.1016/j.telpol.2019.101828

Caputo, A., Pizzi, S., Pellegrini, M. M., & Dabić, M. (2021). Digitalization and business models: Where are we going? A science map of the field. *Journal of BusinessResearch*, 123, 489–501. https://doi.org/10.1016/j.jbusres.2020.09.053

Carlton, M., & Levy, Y. (2015). Expert assessment of the topplatform independent cybersecurity skills for non-IT professionals. *SoutheastCon 2015*. https://doi.org/10.1109/secon.2015.7132932

Checkland, P., & Holwell, S. (1998). *Systemic Practice andAction Research, 11*(1), 9–21. https://doi.org/10.1023/a:1022908820784

Clancey, W. J. (1995). A tutorial on situated learning. In T.-W. Chan & J. Self (Eds.), *Emerging computer technologies in education: Selected papers of the International Conference on Computers and Education* (Taiwan), pp. 49-70 from https://www.researchgate.net

Council of the European Union & European Parliament (2016, April 27). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 april 2016 on the protection of natural persons with regard tothe processing of personal data and on the free movement of such data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (text with EEA Relevance)*. Photo of Publications Office of the European Union. Retrieved February 5, 2023, from https://op.europa.eu/en/publication-detail/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1

Cowan, R. L., & Horan, S. M. (2017). Understanding Information and Communication Technology Use in Workplace Romance Escalation and De-Escalation. International Journal of Business Communication, 58(1), 55–78. https://doi.org/10.1177/2329488417731860

D'Arcy, J., & Hovav, A. (2007). Deterring Internal Information Systems misuse. *Communications of theACM, 50*(10), 113–117. https://doi.org/10.1145/1290958.1290971

Dash, B. & Ansari, M. F. (2022). An Effective CybersecurityAwareness Training Model: First Defense of an Organizational Security Strategy. 9. 2395-0056 from https://www.researchgate.net/

Davis, F. D. (1989). Perceived usefulness, perceived ease ofuse, and user acceptance of Information Technology. *MIS Quarterly, 13*(3), 319. https://doi.org/10.2307/249008

Demek, K. C., Raschke, R. L., Janvrin, D. J., & Dilla, W. N.(2018). DO organizations use a formalized risk management process to address social media risk? *International Journal of Accounting InformationSystems*, 28, 31–44. https://doi.org/10.1016/j.accinf.2017.12.004

Faltermaier, S., Strunk, K., Obermeier, M., & Fiedler, M. (2023, January 3). *Managing organizational cyber security – the distinct role of internalized responsibility*.Handle Proxy. Retrieved February 5, 2023, from https://hdl.handle.net/10125/103373

Goode, J., Levy, Y., Hovav, A., & Smith, J. (2018). Expert assessment of organizational cybersecurity programs anddevelopment of vignettes to measure cybersecurity countermeasures awareness. *Online Journal of Applied Knowledge Management, 6*(1), 67–80. https://doi.org/10.36965/ojakm.2018.6(1)67-80

Hajli, N., & Lin, X. (2016). Exploring the Security of Information Sharing on Social Networking Sites: TheRole of Perceived Control of Information. *Journal of Business Ethics*, 133(1), 111–123. https://doi.org/10.1007/s10551-014-2346-x

Huerta, E., & Jensen, S. (2017). An Accounting InformationSystems Perspective on Data Analytics and Big Data. *The Journal of Information Systems*, 31(3), 101–114. https://doi.org/10.2308/isys-51799

Hutchinson, G., & Ophoff, J. (2020). A Descriptive Review and classification of Organizational Information SecurityAwareness Research. *Information and Cyber Security*, 114–130. https://doi.org/10.1007/978-3-030-43276-8_9

IBM Security Services 2014 cyber security intelligence index.(n.d.). Retrieved February 5, 2023, from http://i.crn.com/sites/default/files/ckfinderimages/userfil es/images/crn/custom/IBMSecurityServices2014.PDF

Jeri-Yabar, A., Sanchez-Carbonel, A., Tito, K., Ramirez- delCastillo, J., Torres-Alcantara, A., Denegri, D., & Carreazo, Y. (2018). Association between Social Mediause (Twitter, Instagram, Facebook) and depressive symptoms: Are Twitter users at higher risk? *International Journal of Social Psychiatry*, 65(1), 14–19.https://doi.org/10.1177/0020764018814270

Kapoor, K. K., Tamilmani, K., Rana, N. P., Patil, P., Dwivedi, Y. K., & Nerur, S. (2017). Advances in socialmedia research: Past, present and future. *Information Systems Frontiers*, 20(3), 531–558. https://doi.org/10.1007/s10796-017-9810-y

Khan, N. F., Ikram, N., Murtaza, H., & Javed, M. (2023). Evaluating Protection Motivation Based Cybersecurity Awareness Training on Kirkpatrick's model. *Computers& Security, 125*, 103049. https://doi.org/10.1016/j.cose.2022.103049

Krings, F., Gioaba, I., Kaufmann, M., Sczesny, S., & Zebrowitz, L. (2021). Older and younger job seekers'impression management on linkedin. *Journal of Personnel Psychology*, 20(2), 61–74. https://doi.org/10.1027/1866-5888/a000269

Landress, A. D., Parrish, J. L., & Terrell, S. (2017). Resiliency as an Outcome of Security Training and Awareness Programs. *AMCIS 2017 Proceedings.* 38. https://aisel.aisnet.org/amcis2017/InformationSystems/P resentations/38

Lara-Cabrera, R., Gonzalez-Pardo, A., & Camacho, D. (2019). Statistical analysis of risk assessment factors andmetrics to evaluate radicalisation in Twitter. *Future Generation Computer Systems*, 93, 971–978. https://doi.org/10.1016/j.future.2017.10.046

Lykou, G., Anagnostopoulou, A., & Gritzalis, D. (2018). Smart airport cybersecurity: Threat mitigation and cyberresilience controls. *Sensors, 19*(1), 19. https://doi.org/10.3390/s19010019

Majmundar, A., Allem, J.-P., Cruz, T. B., & Unger, J. B. (2019). Where do people vape? insights from Twitter data. *International Journal of Environmental Researchand Public Health*, 16(17), 3056. https://doi.org/10.3390/ijerph16173056

Melton, J., Miller, R., & Dunn, P. (2020). Student Social Media Self-evaluation: Addressing the posting paradox in the age of cybervetting. *Journal of Technical Writingand Communication*, 51(3), 273–292. https://doi.org/10.1177/0047281620927014

Miller, R., Parsons, K., & Lifer, D. (2010). Students and social networking sites: The posting paradox. *Behaviour& Information Technology*, 29(4), 377–382. https://doi.org/10.1080/01449290903042491

Morris, A. (2021). Book reviews. *The Velvet Light Trap*, 88,94–108. https://doi.org/10.7560/vlt8809

Nwachukwu, U., Vidgren, J., Niemimaa, M., & Järveläinen, J. (2023, January 3). *Do seta interventions change security behavior? – A literature review*. Handle Proxy.Retrieved February 5, 2023, from https://hdl.handle.net/10125/103396

Oksanen, A., Oksa, R., Savela, N., Kaakinen, M., & Ellonen, N. (2020). Cyberbullying victimization at work: Social Media Identity Bubble Approach. *Computers in HumanBehavior*, 109, 106363. https://doi.org/10.1016/j.chb.2020.106363

Pratama, A. R., Alshaikh, M., & Alharbi, T. (2023). Increasing cybersecurity awareness through situated e-learning: A survey experiment. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4320165

Prodanova, J., & Van Looy, A. (2019). How Beneficial if Social media for Business Process Management? A Systematic Literature Review. *IEEEAccess*, 7, 39583-39599. https://doi.org/10.1109/ACCESS.2019.2903983

Ribeiro-Navarrete, S., Botella-Carrubi, D., Palacios-Marqués, D., & Orero-Blat, M. (2021). The effect of digitalization on business performance: An applied studyof KIBS. *Journal of Business Research*, 126, 319–326. https://doi.org/10.1016/j.jbusres.2020.12.065

Rice, J. C., & Sussan, F. (2016). Digital privacy: A conceptual framework for business. *Journal of PaymentsStrategy & Systems*, 10(3), 260–266.

Rumjaun, A., & Narod, F. (2020). Social Learning theory—Albert Bandura. *Springer Texts in Education*, 85–99. https://doi.org/10.1007/978-3-030-43620-9_7

Sadaghiani-Tabrizi, A. (n.d.). *Revisiting cybersecurity awareness in the midst of disruptions*. ISU ReD: Research and eData. Retrieved February 5, 2023, from https://ir.library.illinoisstate.edu/ijbe/vol163/iss1/6

Sánchez Abril, P., Levin, A., & Del Riego, A. (2012). Blurred Boundaries: Social Media Privacy and the Twenty-First-Century Employee. *American BusinessLaw Journal*, 49(1), 63–124. https://doi.org/10.1111/j.1744-1714.2011.01127.x

Schrameyer, A. R., Graves, T. M., Hua, D. M., & Brandt, N. C. (2016). Online Student Collaboration and FERPAConsiderations. *TechTrends*, 60(6), 540–548. https://doi.org/10.1007/s11528-016-0117-5

Schunk, D. H., & Zimmerman, B. J. (2003). Self-regulationand learning. *Handbook of Psychology*. https://doi.org/10.1002/0471264385.wei0704

Sevignani, S. (2013). The commodification of privacy on theInternet. *Science & Public Policy*, 40(6), 733–739. https://doi.org/10.1093/scipol/sct082

Soens, E., & Claeys, A.-S. (2021). Can Organizations GuideEmployees' social media behavior? the benefits of incentive rather than restrictive social media guidelines.*Journal of Communication Management*, 25(4), 454–471. https://doi.org/10.1108/jcom-02-2021-0017

Sommestad, T., Karlzén, H., & Hallberg, J. (2015). A meta-analysis of studies on Protection Motivation Theory andinformation security behaviour. *International Journal ofInformation Security and Privacy, 9*(1), 26–46. https://doi.org/10.4018/ijisp.2015010102

Wang, S., Kelly, W., & Wang, X. (n.d.). *Hispo: A novel threat analysis and risk mitigation approach to prevent cyber intrusions*. Journal of The Colloquium for Information Systems Security Education. Retrieved from https://cisse.info/journal/index.php/cisse/article/view/35

Warner, K. S. R., & Wäger, M. (2019). Building dynamiccapabilities for digital transformation: An ongoing process of strategic

renewal. *Long Range Planning*, 52(3), 326–349. https://doi.org/10.1016/j.lrp.2018.12.001

Yokoyama, M. H. (2016). How social network sites (SNS) have changed the employer–employee relationship andwhat are the next challenges for human resource (HR)?*REGE - Revista De Gestão*, 23(1), 2–9. https://doi.org/10.1016/j.rege.2015.11.001

Zafar, H., Williams, J., & Gupta, S. (2023, January 3). *Toward an effective SETA program: An Action ResearchApproach*. Handle Proxy. Retrieved February 5, 2023, from https://hdl.handle.net/10125/103036

Zaman, R., & Hassani, M. (2020). On Enabling GDPR Compliance in Business Processes Through Data-DrivenSolutions. *SN Computer Science*, 1(4), 1–15. https://doi.org/10.1007/s42979-020-00215-x

Zurbriggen, E. L., Ben Hagai, E., & Leon, G. (2016). Negotiating privacy and intimacy on Social Media: Review and recommendations. *Translational Issues inPsychological Science*, 2(3), 248–260. https://doi.org/10.1037/tps0000078