KELLEY SCHOOL OF BUSINESS
INDIANA UNIVERSITY

Social networks and social media: Understanding and managing influence vulnerability in a connected society

Patrick F. Bruning [a],*, Bradley J. Alge [b], Hsin-Chen Lin [a]

[a] University of New Brunswick, 255 Singer Hall, 7 Macauley Lane, Fredericton, NB E3B 5A3, Canada
[b] Krannert School of Management, Purdue University, West Lafayette, IN 47907, U.S.A.

Abstract Influence vulnerability has recently become a concern across society and in business. Such vulnerabilities increase as social networks are leveraged by different entities, oftentimes through social media, to affect how we think and behave. While many instances of social influence are positive and beneficial, others can be quite negative and lead to harmful outcomes for organizations and individuals such as reputational damage and an inability to control desirable thoughts, narratives, and behaviors. In general, they can decrease people's freedom of thought and behavior. This article draws on the concepts of social embeddedness and network commitment to outline people's influence vulnerabilities. It then proposes three guidelines to help reduce influence vulnerabilities based on the concepts of trustworthiness, network commitment, and self-management.

1. Maintaining our freedom of thought and action

It is difficult to maintain one's independence of thought and action in societies where our social networks and our connections to them via social media have a profound social influence. The recent Cambridge Analytica scandal (Kleinman, 2018; Wakefield, 2019) and the anti-vaccination movement (BBC News, 2019) are extreme examples of this issue. The Cambridge Analytica scandal is alleged to have influenced major political outcomes in the U.K. and the U.S.—a potent reminder of how vulnerable our most steady institutions are to automated social influence (Kleinman, 2018; Wakefield, 2019). Indeed, the news is full of stories about people being influenced by their social networks, whether relatively impersonal online

* Corresponding author
E-mail addresses: patrick.bruning@unb.ca (P.F. Bruning), algeb@purdue.edu (B.J. Alge), hc.lin@unb.ca (H.-C. Lin)

networks or more personal and intimate relational networks. As a society, we are still adjusting to the molding power of social networking platforms such as Facebook, Instagram, and Twitter. Although a socially connected world presents opportunity, it also poses risks to managers, employees, and other societal members. Social media at its core can expand our exposure to positive, neutral, and negative social forces from our social networks that make us susceptible to social influence. Therefore, the increased prevalence of digital platforms and technologies has amplified the social forces that we face, both online and offline.

Within the business domain, organizations spent $137.63 billion in 2017 on cybersecurity targeted to stop fraudulent activity such as phishing attempts and more general social influence; that spending is expected to reach $167.14 billion by the end of 2019 (Statista, 2019). Third-party software and service firms such as DigitalStakeout, Google Alerts, Hootsuite, Crimson Hexagon, Rankur, TweetDeck, and Reputation.com's Social Suite are used to monitor social media platforms. This monitoring is often employed to look for nefarious attempts by insiders, outsiders, and automated sources to influence a company's reputation. Similar products also exist to protect the reputations of individual people (Smith, 2019). With these technology investments, basic human cognitive and psychological tendencies are often the weakest links in such initiatives (Cellan-Jones, 2019; Dodge, Carver, & Ferguson, 2007; Workman, 2008). Furthermore, many instances of social influence occur through offline interaction. Therefore, managers and societal leaders, as well as workers and other members of society, should proactively self-manage their influence vulnerabilities.

In this regard, our understanding of situations can often be clouded when others attempt to influence social narratives and behaviors. Oftentimes, these influence efforts are driven through social media and personal networks. Bots, artificial intelligence agents, and other social manipulation activities are increasingly infiltrating popular social media platforms to sway people's opinions and influence their behavior (Argo, Grunding, & Vellani, 2019; Brown, 2019; Fisher, 2018). These attempts can sometimes incorporate "fake news" and disinformation (Vosoughi, Roy, & Aral, 2018, p. 1146). Yet, social influence has been a societal concern since well before social media's rise (Asch, 1951; Granovetter, 1985; Janis, 1983), and these offline forms continue to present challenges for managers, employees, and other members of society. Indeed, social influence is a dominant part of work and life that has been amplified as we become more psychologically connected to our social networks through digital platforms.

The idea that social networks can influence peoples' thoughts and behaviors is not new (Berger, 2014; Bond et al., 2012; Brass, Galaskiewicz, Greve, & Tsai, 2004; Granovetter, 1985; Kozinets, de Valck, Wojnicki, & Wilner, 2010). However, the increased use of social media platforms has amplified the forces of social influence. While we know that these threats exist, we are often unsure of how to combat them. This lack of procedural guidance is a vulnerability for organizations and other institutions, as well as for administrators, workers, and other members of society. Therefore, we contribute to the broader discussion on social influence by explaining some critical vulnerabilities brought about by online and offline social influence. While there are many instances of positive social influence (e.g., Ashford, Blatt, & VandeWalle, 2003; Lin, Bruning, & Swarna, 2018; Porter & Woo, 2015), we focus this article on the distinct strategies that people can take to mitigate undesirable and unwanted influence. Indeed, we believe that the process of mitigating vulnerability to harmful or unwanted social influence is quite distinct from increasing exposure to positive influence (Elliot, 1999). Thus, we focus this article on mitigating negative and undesirable forms of influence vulnerability. Herein, we draw on the concepts of social embeddedness and network commitment (Bruning, Alge, & Lin, 2018; Granovetter, 1985) to outline how people become psychologically susceptible to social influence. We then propose proactive strategies based on concepts of trustworthiness (Mayer, Davis, & Schoorman, 1995), network commitment, and self-management (Stewart, Courtright, & Manz, 2011) to help people reduce their influence vulnerability and maintain their freedom of thought and action.

2. Embeddedness and personal influence vulnerability

The topic of social influence and susceptibility lies at the heart of many contemporary managerial concerns. Recent discussions have addressed topics such as the collective protection of privacy (Li, 2019); the implications of social networks on ethical behavior (Key, Azab, & Clark, 2019); the general use of social media for marketing purposes (Berthon, Pitt, Plangger, & Shapiro, 2012; Kaplan & Haenlein, 2010; Kietzmann, Hermkens, McCarthy, & Silvestre, 2011); the influence of social media

communications by brands, opinion leaders, and other consumers (Lin et al., 2018; Lin, Swarna, & Bruning, 2017; Melancon & Dalakas, 2018); inter-organizational communications (Posthuma, Flores, Barlow, & Dworkin, 2018); human attention to contextual information in the digital age (Berthon & Pitt, 2019); and managing employees' emergent online and offline work behavior (Bizzi, 2018; Kim, 2018; Tomczak, Lanzo, & Aguinis, 2018). A central issue within these discussions is social influence, including potential negative influences, which can be derived from our social contexts.

People can become embedded within their social networks, which can create a situation whereby a person becomes fixed within and influenced by their social ties. In this regard, Granovetter (1985) argued that individual behaviors can be influenced by social ties that promote trust and socially desirable behaviors as well as discourage undesirable behaviors. Prior research suggests that embeddedness can serve as a force of employee retention within organizations (Jiang, Liu, McKay, Lee, & Mitchell, 2012; Mitchell, Holtom, Lee, Sablynski, & Erez, 2001). It can also serve, more broadly, as a source of influence over peoples' thoughts and actions (Bond et al., 2012; Bowler & Brass, 2006; Gibbons, 2004; Lawler & Yoon, 1996). Thus, it represents a possible source of vulnerabilities to social influence.

We define *influence vulnerability to one's social network* as a person's susceptibility to being influenced by entities within their social network and broader social environment. These vulnerabilities have a few defining characteristics:

- They are manifest within an individual and represent a generalized susceptibility to being influenced from the person's network, the specific ties within that network, or the broader social environment (Granovetter, 1985; Lawler & Yoon, 1996);

- These vulnerabilities can be manifest within virtual or nonvirtual social interactions, as well as more general patterns of thinking about one's social environment (Bond et al., 2012; Bruning et al., 2018; Gibbons, 2004);

- These vulnerabilities can be derived from a person's psychological experience of embeddedness within their social network or a specific relationship within the network in addition to other dispositional characteristics (Granovetter, 1985; Mayer et al., 1995; Mitchell et al., 2001); and

- They can have positive, neutral, or negative implications (e.g., Jiang et al., 2012; Lin et al., 2018; Vosoughi et al., 2018).

We outline examples of influence vulnerabilities for different personal roles within business and society in Table 1.

We propose that internal or external entities can harness the persuasive power of personal networks to influence the thoughts and behaviors of others. Sometimes these entities are actual direct contacts within a person's network, such as a colleague, a business partner, a boss, or a co-worker (Bowler & Brass, 2006; Gibbons, 2004; Yukl, 2013; Zagenczyk, Scott, Gibney, Murrell, & Thatcher, 2010). Other times, they can be outside parties such as political entities, media outlets, or external competitors that indirectly influence a person by using the person's network contacts as a delivery mechanism (Bond et al., 2012; Lin, 2017; Vosoughi et al., 2018). We focus primarily on peoples' immediate exposure to the social influence via their direct contacts instead of the origin of the influence attempt (which can originate from outside of the network), as more immediate sources should generally have a greater social impact (Latané, 1981).

Research suggests that people become committed to their personal network both as a group of contacts and on a contact-by-contact basis (Bruning et al., 2018; Lawler & Yoon, 1996). According to recent research, peoples' influence vulnerability can be derived from three types of network commitment: (1) *instrumental network commitment* represents the degree to which a person's network connections provide access to nonsubstitutable resources, information, and general value; (2) *normative network commitment* represents the degree to which a person's social connections involve an exchange of favors and information that make the person feel obligated to return the favors to the individuals within the network; and (3) *affective network commitment* represents the degree to which a person's social connections create positive emotional reactions and define a person's identity (Bruning et al., 2018).

The results of this research suggest that compared to people with fewer network contacts, people who are central and have many contacts within their personal network are more susceptible to social influence from a detached outside party. The research found that people were influenced by an experimental manipulation that provided them with the secondhand thoughts and opinions of the network (Bruning et al., 2018). They were also

Table 1. Examples of influence vulnerability according to people's different social roles

Social role	Description of the role	Examples of influence vulnerability for the social role
Organizational or societal administrator	This role involves people who are in a managerial or leadership role within a larger social entity in the corporate, government, or not-for-profit sectors. It can also include informal leaders within other formal/informal collectives and societies.	External competitors attempting to harm or interfere with strategic organizational decision-making.
		Internal competitors attempting to sabotage or harm the quality of a person's decision-making to gain relative favor for promotion or broader prestige.
		Subordinates and followers trying to influence decisions to gain personally favorable outcomes.
		Non-subordinate stakeholders trying to influence decisions to gain personally favorable outcomes.
		Internal or external actors trying to influence decisions to promote competing ideologies and logics.
Organizational worker	This role involves people who work, or otherwise contribute, in a non-supervisory capacity. People filling this role can be paid employees or unpaid volunteers. They can contribute to social entities within the corporate, government, or not-for-profit sectors. This role can be held by supervisory workers when they are engaging in their non-supervisory work.	Leaders and managers trying to influence a person's motivations and behaviors to gain greater productivity and commitment.
		Internal or external actors trying to influence motivations and beliefs to promote competing ideologies and logics.
		Internal or external entities trying to gain access to private and secure organizational information.
		External competitors attempting to interfere with a worker's productivity and commitment within their host organization.
		Internal competitors attempting to sabotage or harm the quality of a person's work to gain relative favor for promotion or broader prestige.
		External customers, clients, or other stakeholders trying to influence a worker's decision-making to gain personally favorable outcomes.

Table 1 (*continued*)

Social role	Description of the role	Examples of influence vulnerability for the social role
Consumer or constituent	This role involves people within society who can be engaged by companies and other social entities to purchase products and services, provide support or patronage to a social entity, or otherwise adopt or accept a social message.	Companies trying to convince consumers to purchase their products or services.
		Companies and other social entities trying to promote the awareness and appeal of their brands.
		Political entities trying to convince consumers to support their candidacy or social mission.
		Political entities trying to convince consumers to reject the candidacy or social mission of a competing entity.
		Social entities trying to gain greater awareness and non-commercial support, such as volunteering, lobbying, or word-of-mouth, from consumers.
		Governments and other social entities trying to alter the thoughts and behaviors of their constituents.
Member of society	This role involves people within society who are in a position to communicate or otherwise interact with other people within one or more societies. Their relationships can be part of broader familial, friendship, interest-based, or other informal social networks within society.	People within society trying to convince others to give them economic resources.
		People within society trying to convince others to give them greater social status and prestige.
		People within society trying to convince others to give them allegiance within informal social competitions.
		People trying to alter the different thoughts and behaviors of others.
		People or other entities trying to gain access to private information.
		People within society trying to convince others to support a third-party political entity or social mission.

Note: The table above outlines examples of different social roles that people hold within society and some general types of potentially negative influence attempts they can be subject to within these roles. The roles are organized according to people's affiliation with and status within different social entities. Therefore, many people are likely to hold two or more of these roles. The examples of potential influence attempts are presented to give descriptive examples and are not intended to be an exhaustive list or typology. Many of these examples of influence are not decisively negative, however, each of them can be perceived as negative and undesirable for certain people under certain circumstances. Therefore, each example holds the potential to be negative and/or undesirable.

influenced directly by the individual members of their personal networks. These relationships were found to occur according to the person's sense of status and positive feelings associated with their network connections, suggesting that they became vulnerable as they embraced and enjoyed their status. The research also suggested that people became susceptible to social influence from their network ties because of perceived dependence and reciprocal obligation.

The general findings that network commitments increase a person's influence vulnerability align with previous research that suggests our social networks and social environments influence how we think and behave (Gibbons, 2004; Latané, 1981; Zagenczyk et al., 2010). They also align with the generalized finding that different types and targets of commitment make a person vulnerable to influence from the entities and ideas to which they are committed (Hershcovitch & Meyer, 2002; Klein, Molloy, & Brinsfield, 2012; Klein, Wesson, Hollenbeck, & Alge, 1999; Kukenberger, Mathieu, & Ruddy, 2015; Meyer, Allen, & Smith, 1993; Meyer, Morin, & Vandenberghe, 2015; Monnot, Wagner, & Beehr, 2011; Weng & McElroy, 2012). Furthermore, research suggests that social media could be a functional delivery mechanism of this social influence (Bond et al., 2012; Vosoughi et al., 2018). Together, these findings support the idea that people's social embeddedness and network commitments can make them vulnerable to online and offline social influence.

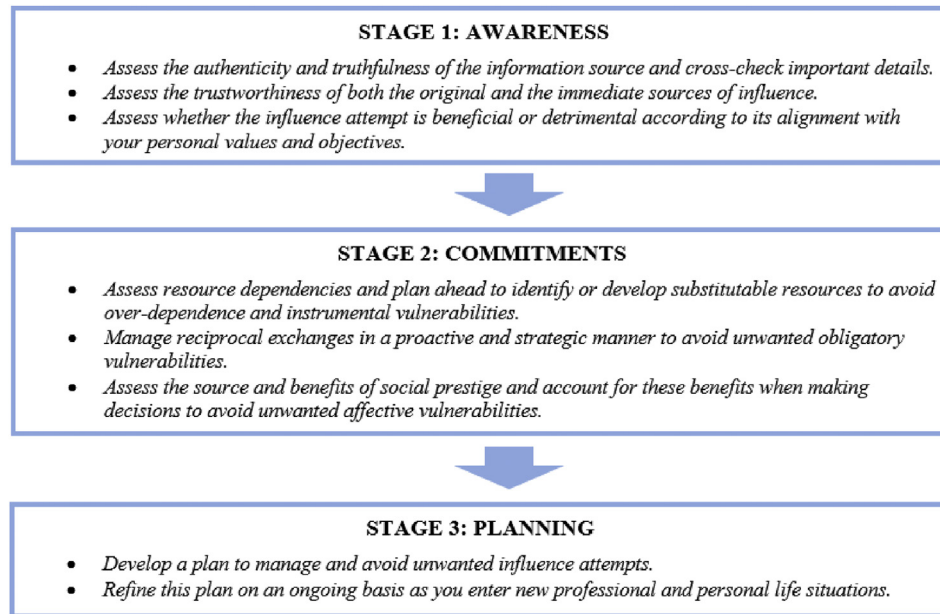## 3. Implications of personal influence vulnerability

Influence attempts can originate within a person's network or could come from an outside party that harnesses the person's network connections to infiltrate and gain access to them. For example, these attempts can come from managers, employees, colleagues, friends, family, and competitors, as well as other known and unknown social entities. Whether positive or negative, these influence attempts can profoundly affect individual and organizational decisions and possibly threaten their reputations, leadership effectiveness, work quality, and information security as examples. In cases of detrimental social influence, people could

abandon critical thinking in favor of the prevailing winds of one's social networks (Janis, 1983).

Influence vulnerability has implications for executives, managers, and other administrators, as well as for employees and other members of society. Given the specific findings that high-status individuals can become vulnerable to social influence according to their centrality within and attachment to their networks (Bruning et al., 2018), the research has clear implications for prominent decision makers. There is a popular belief that people can access more power and freedom as they gain status in an organization or broader society and this logic is reinforced by the research on power, social networks, and influence (Chiu, Balkundi, & Weinberg, 2016; Lin, 2017; Mehra, Kilduff, & Brass, 2001). However, previous findings on network commitment suggest that this prestige might also make people more susceptible to being influenced by the people that they interact with, as well as other people who might harness the social network as a social influence tactic (Bruning et al., 2018). This susceptibility could make executives and managers particularly vulnerable. On the one hand, they have noticeable power and freedom to do what they want, which could give them a false sense of security. On the other hand, their sense of prestige could make them more vulnerable to subtle—and possibly unexpected—influence attempts. These attempts could lead to faulty decision-making that could harm the organization's reputation, leadership, and security according to the specifics of the decisions made (Kish-Gephart, Harrison, & Trevino, 2010; Schaubroeck et al., 2012). These vulnerabilities could become even more exposed as the social aspects of work and life become increasingly digitized. Social influence can now be programmed, automated, and artificially amplified, making this increased exposure a current reality (Bond et al., 2012; Vosoughi et al., 2018).

These sources of influence vulnerability should also be considered for general workers and members of society (Bond et al., 2012; Gibbons, 2004; Vosoughi et al., 2018; Zagenczyk et al., 2010). Within broader nonmanagerial work and personal contexts, these principals can apply to how people navigate the webs of social influence that they encounter through their professional and nonprofessional personal networks. In some cases, it can benefit people to be influenced socially. As members of work teams comprised of other diligent and

Figure 1. Stages of proactive influence vulnerability management

```
┌─────────────────────────────────────────────────────────────────┐
│                    STAGE 1: AWARENESS                             │
│  • Assess the authenticity and truthfulness of the information   │
│    source and cross-check important details.                     │
│  • Assess the trustworthiness of both the original and the       │
│    immediate sources of influence.                               │
│  • Assess whether the influence attempt is beneficial or         │
│    detrimental according to its alignment with your personal     │
│    values and objectives.                                        │
└─────────────────────────────────────────────────────────────────┘
                               ▼
┌─────────────────────────────────────────────────────────────────┐
│                   STAGE 2: COMMITMENTS                            │
│  • Assess resource dependencies and plan ahead to identify or    │
│    develop substitutable resources to avoid over-dependence and  │
│    instrumental vulnerabilities.                                 │
│  • Manage reciprocal exchanges in a proactive and strategic      │
│    manner to avoid unwanted obligatory vulnerabilities.          │
│  • Assess the source and benefits of social prestige and account │
│    for these benefits when making decisions to avoid unwanted    │
│    affective vulnerabilities.                                    │
└─────────────────────────────────────────────────────────────────┘
                               ▼
┌─────────────────────────────────────────────────────────────────┐
│                    STAGE 3: PLANNING                             │
│  • Develop a plan to manage and avoid unwanted influence         │
│    attempts.                                                      │
│  • Refine this plan on an ongoing basis as you enter new         │
│    professional and personal life situations.                    │
└─────────────────────────────────────────────────────────────────┘
```

Note: The figure above outlines considerations that people should make when evaluating their influence vulnerabilities. These considerations are presented in sequence to help people ensure that they have completed the appropriate background work for each step in their decision-making and planning. As multiple iterations of the process will be likely, the stages may also be parallel and simultaneous. Evaluations and decisions might also need to be revised whereby one revisits earlier considerations.

innovative workers, a person might learn to work harder and to adopt new innovative work practices as a result of social learning and attempts to align with the norms of the group (Ashford et al., 2003; Bruning & Campion, 2018, 2019). People can also be influenced to act in a more ethical manner (Kish-Gephart et al., 2010), and they can actively seek online opinion leaders and other sources of information to gain important functional information about certain products and services (Kozinets et al., 2010; Lin et al., 2018; Lin & Kalwani, 2018).

However, there can also be activities, dialogues, and associated subgroups that could threaten a person's career success, ethical conduct, contributions to collective security, and personal well-being. There can be subgroups within organizations and society that promote professionally or personally compromising objectives that many people would want to avoid as a source of influence (Felps et al., 2009; Kish-Gephart et al., 2010). People can also be exposed to prominent influence from online social networks (Bond et al., 2012). In some cases, this exposure can make them susceptible to revealing confidential information or spreading disinformation (Dodge et al., 2007; Vosoughi et al., 2018; Workman, 2008). Social influence is often immediately accessible in a digitally connected world. Individuals can take the first steps in exerting more self-control over their influence vulnerability to help protect their independence of thought and action.

4. Guidelines for mitigating influence vulnerability

Companies, employees, and other members of society need strategies to manage their influence vulnerability since it can have negative implications. The guidelines presented herein primarily focus on mitigating potentially harmful vulnerabilities as capitalizing on opportunities could follow a somewhat different process (Ashford et al., 2003; Elliot, 1999; Lin & Kalwani, 2018). We will, however, bring the possibility of opportunities back into consideration when outlining elements that should be considered when developing plans to mitigate influence vulnerability. We outline a multistage framework that is organized according to three sequential principles to help people mitigate their influence vulnerabilities (Figure 1). The format of this figure is organized using a structure similar to the recently published multistage sequence of managing online opinion leaders (Lin et al., 2018). First, we propose that people develop their awareness of influence vulnerability. This awareness involves subcomponent assessments of trustworthiness and trust

(Mayer et al., 1995), and alignment with one's personal objectives (Stewart et al., 2011). Second, we propose that people evaluate and manage their commitments proactively. This cognitive self-management specifically involves focused activities of managing one's instrumental, normative, and affective network commitments to decrease unwanted influence vulnerability that is derived from social embeddedness (Bruning et al., 2018; Granovetter, 1985). Finally, we propose that people engage in proactive planning by creating and revising a systematic strategy for self-managing one's influence vulnerabilities (Stewart et al., 2011). This self-management could involve deciding when to change one's network commitments or even network configurations.

In this framework, we treat the sources of vulnerability that people should consider according to their awareness (i.e., authentication, trustworthiness, and alignment) as being distinct from the vulnerabilities derived from network commitments. The threats posed by a lack of authenticity and trustworthiness of a social contact within a social influence context would likely represent a generalized vulnerability to deceit. Alignment represents the person's awareness of whether an influence attempt should be accepted or rejected according to its congruence with their objectives (Stewart et al., 2011). Network commitment accounts for peoples' acquiescence to coercion, pressure, ingratiation, and other tactics (Yukl, 2013) that could be either intentional or unintentional on the part of the influencer. In this regard, people can be consciously vulnerable to their closest and most trusted contacts (Latané, 1981; Lawler & Yoon, 1996). Therefore, whereas authentication, trustworthiness, and alignment help a person to become aware of latent threats, network commitments represent vulnerabilities that are derived from motivational forces within a person. The proposed guidelines are further summarized in an applied checklist, derived from Figure 1, to help people mitigate their influence vulnerabilities by considering specific questions (Table 2).

4.1. Be aware of influence vulnerabilities and decide which thoughts, decisions, and actions are most important to protect from being influenced

Social influence is powerful partly because as it unfolds, people can be unaware that it is happening. Thus, a first step toward guarding against unwanted influence is to be aware of the situations in which other people might want to influence us. In this regard, proactive influence attempts occur when another person or group tries to change or influence one's cognitions, beliefs, and behaviors (Yukl, 2013). As broader societal consumers, these situations could also occur any time a person intentionally or unintentionally seeks outside information that benefits them (Ashford et al., 2003; Lin et al., 2018; Lin & Kalwani, 2018). Given the wide variety of situations in which people can be influenced socially, they will experience trade-offs between cognitive effort, relational maintenance, and threats to their autonomy when deciding which influence attempts to avoid.

To address the undesirable vulnerabilities posed by social influence within a broader plan of action, a person must consider the general vulnerabilities that they have to social influence. This assessment should be engaged according to the specific sources of influence for which they can be vulnerable, the situations in which they might be the most vulnerable, and the situations in which the individual and collective implications of this vulnerability could be the most detrimental. The first part of this process is to decide whether the source of information is legitimate—are the people who they say they are? Since an influence attempt can originate from outside of a person's network, this assessment should be made for both immediate sources of the influence attempt and the original sources of these attempts. While authentication might be relatively straightforward when we engage in-person communications with people that we know, online communications present more opportunities for deceit. Given this potential for deceit, some online platforms do authenticate their members (Lin, 2017) and this authentication should be sought vigilantly when gathering information from an unknown party. People should also cross-validate the information that they receive, given the aggressive way that disinformation can diffuse through a network (Vosoughi et al., 2018).

The second part of this process would involve assessing the trustworthiness of the source of the influence attempt. This assessment should consider aspects of ability, benevolence, and integrity, which should all be apparent to a reasonable degree for a source to be considered trustworthy (Mayer et al., 1995).

Assessments of ability would consider whether one believes that the sources can capably provide accurate information. *Assessments of benevolence* would consider whether one believes that the sources have the person or their general followers' best interests in mind. *Assessments of integrity* would consider any perceptions that one might

Table 2. A procedural checklist for proactive influence vulnerability management

Guideline # 1	Be aware of influence vulnerabilities and decide which thoughts, decisions, and actions are most important to protect from being influenced.	__ Are the person or people who I encounter, including virtual interactions on e-mail and social media, actually who they claim that they are?
		__ Are the person or people who I encounter capable of providing accurate information, do they have me or their followers' best interests in mind, and do they have high integrity on issues relevant to what they are communicating?
		__ In my work or personal life domains, what are the situations where other people will try to get me to do certain things or think in certain ways, or conversely, not do certain things or not think certain ways?
		__ Of these situations at work and in my personal life, which of them are uncomfortable, unethical, and otherwise detrimental?
		__ Are these seemingly uncomfortable, unethical, or detrimental requests reasonable, responsible, and necessary from the point of view of the person making the request?
Guideline #2	Proactively manage network commitments to decrease unwanted influence vulnerability.	__ In my work or personal life domains, who are the people that are the most non-substitutable in the fulfillment of my most critical needs?
		__ Are there people or groups in my work or personal life domains that I feel dependent on who either do not fulfill a critical need, or who are substitutable, that also try to influence me to do things that are uncomfortable, unethical, and otherwise detrimental?
		__ In my work or personal life domains, who are the people or groups that I feel the strongest sense of obligation towards?
		__ Are there people or groups in my work or personal life domains that I feel a strong obligation towards that might not hold a similarly strong obligation towards me and that are not as committed to the relationship as I am, but that also try to influence me to do things that are uncomfortable, unethical, and otherwise detrimental?
		__ In my work or personal life domains, who are the people or groups that make me feel valuable and important?
		__ Are there people or groups in either my work or personal life domains that make me feel valuable or important, but that also try to influence me to do things that are uncomfortable, unethical, and otherwise detrimental?
Guideline #3	Create a proactive plan to understand and manage influence vulnerability.	__ Begin with a focus on your awareness and evaluation of your possible vulnerabilities to social influence that could be harmful or otherwise misaligned with your objectives (i.e., Guideline 1).
		__ Specifically assess your vulnerabilities to social influence according to dependence, obligation, and pride (i.e., Guideline 2).
		__ Outline your ways of reducing specific vulnerabilities that are uncomfortable, unethical, and otherwise detrimental (i.e., Guidelines 1 and 2).
		__ This plan should be considered on an ongoing basis and as you enter new life situations to help you better manage your own cognitive and behavioral autonomy in your most important work and personal life domains.

Note: The table above is intended to provide specific questions or objectives that a person can address while engaging the different stages of proactive influence vulnerability management presented in Figure 1.

have about the source's general moral integrity that are relevant to the information that they are communicating.

In this regard, authentication can be one of the multiple indicators of integrity (Lin, 2017). It is also important to account for one's disproportional tendency to trust people as this will influence how a source's trustworthiness translates to the trust that a person holds for the source (Mayer et al., 1995). Moreover, people often do not get information from the original source on social media, as it often has been shared via an online network (Bond et al., 2012; Vosoughi et al., 2018). The trustworthiness of the source should also be evaluated because even reputable outlets can make authentication difficult when they quote anonymous sources. Audiences can overlook this lack of clear authentication when they are presented by a legitimate outlet. Yet, even these legitimate outlets are not immune to ill-intended leaks of bogus information from their anonymous sources.

In addition to considering the source of the information, individuals must also pay attention to the situations in which they are most vulnerable to social influence that could pose threats for themselves or others. Therefore, a third consideration involves identifying the situations in which other people will try to influence a person's thoughts and behaviors in potentially undesirable ways (see Table 1 for generalized examples). Influence attempts can be aligned with a person's idiosyncratic objectives and, therefore, represent environmental events that should either be approached or avoided (Elliot, 1999; Stewart et al., 2011). Not every instance of social influence is problematic. Some instances are inconsequential while others will present beneficial opportunities. Other times, the influence attempt is necessary within a broader system of collective organizing, whereby individuals must trade off some of their own wishes to facilitate group success and relational viability (Burns, 1978; Granovetter, 1985). However, from a risk-management perspective, it would benefit peoples' work and personal lives to identify and understand when influence vulnerability is most threatening. This potential for goal alignment would represent one of the multiple indicators of benevolence. Once a person has outlined the situations in which social influence is possible, one should identify the undesirable influence attempts according to the implications and the alignment with the person's objectives.

4.2. Proactively manage one's network commitments to decrease unwanted influence vulnerability

People can still be vulnerable to social influence attempts even when they are aware of their vulnerabilities (Bowler & Brass, 2006; Granovetter, 1985; Lawler & Yoon, 1996). This vulnerability can be derived from the person's social embeddedness and the psychological bonds that people have within their personal networks. In this regard, people could be influenced to do something that they know might not be the right or best thing to do based on their instrumental dependencies, reciprocal obligations, and enjoyment of social prestige (Bruning et al., 2018). This guideline will involve three distinct sets of recommendations according to the instrumental, normative, and affective types of network commitment.

First, people should be aware of resource dependencies and prepare to identify or develop substitutable resources to avoid overdependence and instrumental vulnerabilities. The concept of instrumental network commitment is based on peoples' needs and their dependence on members of their network to help support these needs (Bruning et al., 2018). When a person senses that they have only a few alternative sources of need fulfillment, they become more closely bound to any given contact that they have who can support these particular needs. This makes them susceptible to influence according to their dependence on a wide range of social resources (Foa, 1971). While it might be impossible to completely reduce such dependencies, people can be aware of them and minimize them by only deciding to feel dependent on the contacts that are the most non-substitutable, and least harmful, sources of the fulfillment of the person's most critical needs.

Second, people should manage reciprocal exchanges proactively and strategically to avoid unwanted obligatory vulnerabilities. The concept of normative network commitment is based on peoples' reciprocal obligations towards members of their network as part of an ongoing social exchange (Bruning et al., 2018). When a person senses that they are bound by an obligation to reciprocate or to give back to another person or group, they become susceptible to influence from this person or group according to their sense of obligation. While social exchanges are a central and often necessary part of our work and personal lives (Cropanzano & Mitchell, 2005), they also represent a possible vulnerability to social influence (Bruning et al., 2018). Thus, they should be

evaluated and managed vigilantly to ensure that our strongest obligations are focused on those contacts who reciprocate this obligation and are similarly committed to the relationship.

Third, people should be aware of the sources and benefits of social prestige, and account for these benefits, when making decisions to avoid unwanted affective vulnerabilities. The concept of affective network commitment is based on peoples' sense of prestige and identification with their network of social contacts (Ashforth & Mael, 1989; Bruning et al., 2018). When a person senses that they are held with high prestige by others and that these relationships help define ones' self, the person can become vulnerable to social influence due to identification and pride. Experiences of pride, confidence, and the knowledge that one is valued by others are important predictors of work performance and personal well-being (Judge & Bono, 2001; Judge, Erez, Bono, & Thoresen, 2003). However, people must also be careful not to be blindly influenced in an unwanted manner by this prestige.

4.3. Create a plan to understand and manage influence vulnerability on an ongoing basis

To be prepared for either expected or unexpected influence attempts, people and organizations should try to create proactive plans to manage and mitigate their unwanted and detrimental influence vulnerabilities (Stewart et al., 2011). These plans should be strategic and should begin with an outline of the possible influence vulnerabilities. At this phase, it is important to remember that social influence can have positive benefits. Therefore, it is important to be aware of the opportunities as well as the threats presented by social influence when developing or refining one's plan (Mayer et al., 1995). Once these opportunities and threats have been outlined, a person should then specifically assess their influence vulnerability according to dependence, obligation, and pride. With this information in mind, one should outline possible ways of reducing the vulnerabilities that are uncomfortable, unethical, and otherwise detrimental to ones' self, organization, or society. Finally, this plan should be evaluated and revised on an ongoing basis and as a person enters new professional and personal life situations. These modifications will help them to better manage their own cognitive and behavioral autonomy over time (Stewart et al., 2011).

While the idea of planning, monitoring, and correcting one's influence vulnerabilities is likely to be self-evident, many people make critical mistakes while doing routine tasks that have not been formalized into a systematic process. The potential for these mistakes further increases when people are less aware of the scope, pattern, and specific threats posed by their wide array of influence vulnerabilities. Additionally, these mistakes increase even more when people make quick and automatic decisions as often occur when scanning different social media platforms. Therefore, we suggest the third guideline to address the fact that merely being aware of vulnerabilities is not a sufficient solution to mitigating against these vulnerabilities being actualized in real threats. In this regard, people are recommended to systematically organize and even map out their influence vulnerabilities according to their specific societal roles (see Table 1 for examples of these roles and associated vulnerabilities), and then adjust this organizing mechanism as their lives, roles, and influence vulnerabilities change. This proactive organization can also help people understand, derive, and even mentally rehearse the proactive self-management tactics that they can use to combat these unwanted influence vulnerabilities.

5. Concluding thoughts

We describe how people can be vulnerable to influence from their social networks, according to trustworthiness, social embeddedness, and network commitment. We then propose procedural guidelines to help people mitigate these vulnerabilities. While we have focused primarily on mitigating vulnerability and threats that can come from undesirable forms of social influence, numerous opportunities and benefits can come from social influence. Therefore, future research should develop applied procedural frameworks that can explain how to cultivate, enhance, and benefit from positive forms of social influence. For example, organizations might leverage the power of social networks to drive organization-wide acceptance of change efforts. This future research should also develop more detailed procedural frameworks for addressing the specific challenges involved with mitigating influence vulnerabilities. In conclusion, we suggest that people think closely about their exposure to social influence as a result of their membership in social networks, whether or not this influence can pose a threat, and how they can mitigate negative influence vulnerabilities through systematic planning. Also, while the proactive management of influence vulnerabilities occurs within individual people,

organizations and societies can reinforce more effective proactive management of influence vulnerabilities within their employees and constituents. Here, they could run awareness campaigns; and offer training on the proactive self-management of influence vulnerabilities.

References

Argo, C., Grunding, T., & Vellani, N. (2019, February 8). Social engineering is the new method of choice for hackers. Here's how it works. *CBC*. Available at https://www.cbc.ca/news/technology/marketplace-social-engineering-sim-swap-hack-1.5009279

Asch, S. E. (1951). Effects of group pressure upon the modification and distortion of judgment. In H. Guetzkow (Ed.), *Groups, leadership, and men* (pp. 177–190). Pittsburgh, PA: Carnegie Press.

Ashford, S. J., Blatt, R., & VandeWalle, D. (2003). Reflections on the looking glass: A review of research on feedback-seeking behavior in organizations. *Journal of Management, 29*(6), 773–799.

Ashforth, B. E., & Mael, F. (1989). Social identity theory and the organization. *Academy of Management Review, 14*(1), 20–39.

BBC News. (2019, March 5). *US teen who defied parents over vaccine warns of misinformation*. Available at https://www.bbc.com/news/world-us-canada-47449517

Berger, J. (2014). Word of mouth and interpersonal communication: A review and directions for future research. *Journal of Consumer Psychology, 24*(4), 586–607.

Berthon, P. R., & Pitt, L. F. (2019). Types of mindfulness in an age of digital distraction. *Business Horizons, 62*(2), 131–137.

Berthon, P. R., Pitt, L. F., Plangger, K., & Shapiro, D. (2012). Marketing meets Web 2.0, social media, and creative consumers: Implications for international marketing strategy. *Business Horizons, 55*(3), 261–271.

Bizzi, L. (2018). The hidden problem of Facebook and social media at work: What if employees start searching for other jobs? *Business Horizons, 61*(1), 23–33.

Bond, R. M., Fariss, C. J., Jones, J. J., Kramer, A. D., Marlow, C., Settle, J. E., et al. (2012). A 61-million-person experiment in social influence and political mobilization. *Nature, 489*, 295–298.

Bowler, W. M., & Brass, D. J. (2006). Relational correlates of interpersonal citizenship behavior: A social network perspective. *Journal of Applied Psychology, 91*(1), 70–82.

Brass, D. J., Galaskiewicz, J., Greve, H. R., & Tsai, W. (2004). Taking stock of networks and organizations: A multilevel perspective. *Academy of Management Journal, 47*(6), 795–817.

Brown, J. (2019, July 9). How social media could ruin your business. *BBC*. Available at https://www.bbc.com/news/business-48871456

Bruning, P. F., Alge, B. J., & Lin, H.-C. (2018). The embedding forces of network commitment: An examination of the psychological processes linking advice centrality and susceptibility to social influence. *Organizational Behavior and Human Decision Processes, 148*, 54–69.

Bruning, P. F., & Campion, M. A. (2018). A role-resource approach-avoidance model of job crafting: A multi-method integration and extension of job crafting theory. *Academy of Management Journal, 61*(2), 499–522.

Bruning, P. F., & Campion, M. A. (2019). Exploring job crafting: Diagnosing and responding to the ways employees adjust their jobs. *Business Horizons, 62*(5), 625–635.

Burns, J. M. (1978). *Leadership*. New York, NY: Harper & Row.

Cellan-Jones, R. (2019, February 16). Was Jeff Bezos the weak link in cyber-security? *BBC*. Available at https://www.bbc.com/news/technology-47253869?intlink_from_url=https://www.bbc.com/news/topics/cz4pr2gd85qt/cyber-security&link_location=live-reporting-correspondent

Chiu, C.-Y., Balkundi, P., & Weinberg, F. J. (2016). When managers become leaders: The role of manager network centralities, social power, and followers' perception of leadership. *Leadership Quarterly, 28*(2), 334–348.

Cropanzano, R., & Mitchell, M. S. (2005). Social exchange theory: An interdisciplinary review. *Journal of Management, 31*(6), 874–900.

Dodge, R. C., Carver, C., & Ferguson, A. J. (2007). Phishing for user security awareness. *Computers & Security, 26*(1), 73–80.

Elliot, A. J. (1999). Approach and avoidance motivation and achievement goals. *Educational Psychologist, 34*(3), 169–189.

Felps, W., Mitchell, T. R., Hekman, D. R., Lee, T. W., Holtom, B. C., & Harman, W. S. (2009). Turnover contagion: How coworkers' job embeddedness and job search behaviors influence quitting. *Academy of Management Journal, 52*(3), 545–561.

Fisher, M. (2018, November 7). Social media's re-engineering effect, from Myanmar to Germany. *New York Times*. Available at https://www.nytimes.com/2018/11/07/technology/personaltech/social-media-effect-myanmar-germany.html

Foa, U. (1971). Interpersonal and economic resources. *Science, 171*(3969), 345–351.

Gibbons, D. E. (2004). Friendship and advice networks in the context of changing professional values. *Administrative Science Quarterly, 49*(2), 238–262.

Granovetter, M. (1985). Economic action and social structure: The problem of embeddedness. *American Journal of Sociology, 91*(3), 481–510.

Hershcovitch, L., & Meyer, J. P. (2002). Commitment to organizational change: Extension of a three-component model. *Journal of Applied Psychology, 87*(3), 474–487.

Janis, I. L. (1983). *Groupthink: Psychological studies of policy decisions and fiascos*. Boston, MA: Houghton Mifflin Company.

Jiang, K., Liu, D., McKay, P. F., Lee, T. W., & Mitchell, T. R. (2012). When and how is job embeddedness predictive of turnover? A meta-analytic investigation. *Journal of Applied Psychology, 97*(5), 1077–1096.

Judge, T. A., & Bono, J. E. (2001). Relationship of core self-evaluations traits—self-esteem, generalized self-efficacy, locus of control, and emotional stability—with job

satisfaction and job performance: A meta-analysis. *Journal of Applied Psychology, 86*(1), 80–92.

Judge, T. A., Erez, A., Bono, J. E., & Thoresen, C. J. (2003). The core self-evaluations scale: Development of a measure. *Personnel Psychology, 56*(2), 303–331.

Kaplan, A. M., & Haenlein, M. (2010). Users of the world unite! the challenges and opportunities of social media. *Business Horizons, 53*(1), 59–68.

Key, T. M., Azab, C., & Clark, T. (2019). Embedded ethics: How complex systems and structures guide ethical outcomes. *Business Horizons, 62*(3), 327–336.

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.

Kim, S. (2018). Managing millennials' personal use of technology at work. *Business Horizons, 61*(2), 261–270.

Kish-Gephart, J. J., Harrison, D. A., & Trevino, L. K. (2010). Bad apples, bad cases, and bad barrels: Meta-analytic evidence about sources of unethical decisions at work. *Journal of Applied Psychology, 95*(1), 1–31.

Kleinman, Z. (2018, March 21). Cambridge Analytica: The story so far. *BBC*. Available at https://www.bbc.com/news/technology-43465968

Klein, H. J., Molloy, J. C., & Brinsfield, C. T. (2012). Reconceptualizing workplace commitment to redress a stretched construct: Revisiting assumptions and removing confounds. *Academy of Management Review, 37*(1), 130–151.

Klein, H. J., Wesson, M. J., Hollenbeck, J. R., & Alge, B. J. (1999). Goal commitment and the goal-setting process: Conceptual clarification and empirical synthesis. *Journal of Applied Psychology, 84*(6), 885–896.

Kozinets, R. V., de Valck, K., Wojnicki, A. C., & Wilner, S. J. S. (2010). Networked narratives: Understanding word-of-mouth marketing in online communities. *Journal of Marketing, 74*(2), 71–89.

Kukenberger, M. R., Mathieu, J. E., & Ruddy, T. (2015). A cross-level test of empowerment and process influences on members' informal learning and team commitment. *Journal of Management, 41*(3), 987–1016.

Latané, B. (1981). The psychology of social impact. *American Psychologist, 36*(4), 343–356.

Lawler, E. J., & Yoon, J. (1996). Commitment in exchange relations: Test of a theory of relational cohesion. *American Sociological Review, 61*(1), 89–108.

Li, D. (2019). It takes a village to protect privacy. *Business Horizons, 62*(1), 1–3.

Lin, H.-C. (2017). How political candidates' use of Facebook relates to the election outcomes. *International Journal of Market Research, 59*(1), 77–96.

Lin, H.-C., Bruning, P. F., & Swarna, H. (2018). Using online opinion leaders to promote the hedonic and utilitarian value of products and services. *Business Horizons, 61*(3), 431–442.

Lin, H.-C., & Kalwani, M. U. (2018). Culturally contingent electronic word-of-mouth signaling and screening: A comparative study of product reviews in the United States and Japan. *Journal of International Marketing, 26*(2), 80–102.

Lin, H.-C., Swarna, H., & Bruning, P. F. (2017). Taking a global view on brand post popularity: Six social media brand post practices for global markets. *Business Horizons, 60*(5), 621–633.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review, 20*(3), 709–734.

Mehra, A., Kilduff, M., & Brass, D. J. (2001). The social networks of high and low self-monitors: Implications for workplace performance. *Administrative Science Quarterly, 46*(1), 121–146.

Melancon, J. P., & Dalakas, V. (2018). Consumer social voice in the age of social media: Segmentation profiles and relationship marketing strategies. *Business Horizons, 61*(1), 157–167.

Meyer, J. P., Allen, N. J., & Smith, C. A. (1993). Commitment to organizations and occupations: Extension and test of a three-component conceptualization. *Journal of Applied Psychology, 78*(4), 538–551.

Meyer, J. P., Morin, A. S., & Vandenberghe, C. (2015). Dual commitment to organization and supervisor: A person-centered approach. *Journal of Vocational Behavior, 88*, 56–72.

Mitchell, T. R., Holtom, B. C., Lee, T. W., Sablynski, C. J., & Erez, M. (2001). Why people stay: Using job embeddedness to predict voluntary turnover. *Academy of Management Journal, 44*(6), 1102–1121.

Monnot, M. J., Wagner, S., & Beehr, T. A. (2011). A contingency model of union commitment and participation: Metaanalysis of the antecedents of militant and nonmilitant activities. *Journal of Organizational Behavior, 32*(8), 1127–1146.

Porter, C. M., & Woo, S. E. (2015). Untangling the networking phenomenon: A dynamic psychological perspective on how and why people network. *Journal of Management, 41*(5), 1477–1500.

Posthuma, R. A., Flores, G. L., Barlow, M. A., & Dworkin, J. B. (2018). Social signaling and interorganizational relationships: Lessons from the professional sports industry. *Business Horizons, 61*(4), 521–531.

Schaubroeck, J. M., Hannah, S. T., Avolio, B. J., Kozlowski, S. W. J., Lord, R., Trevino, L. K., et al. (2012). Embedding ethical leadership within and across organizational levels. *Academy of Management Journal, 55*(5), 1053–1078.

Smith, M. (2019, September 6). The secrets of controlling your internet profile. *BBC*. Available at https://www.bbc.com/news/business-49006256

Statista. (2019, March 4). *Size of the cybersecurity market worldwide, from 2017 to 2023*. Available at https://www.statista.com/statistics/595182/worldwide-security-as-a-service-market-size/

Stewart, G. L., Courtright, S. H., & Manz, C. C. (2011). Self-leadership: A multilevel review. *Journal of Management, 37*(1), 185–222.

Tomczak, D. L., Lanzo, L. A., & Aguinis, H. (2018). Evidence-based recommendations for employee performance monitoring. *Business Horizons, 61*(2), 251–259.

Vosoughi, R., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science, 359*(6380), 1146–1151.

Wakefield, J. (2019, February 18). Facebook needs regulation as Zuckerberg 'fails' — UK MPs. *BBC*. Available at https://www.bbc.com/news/technology-47255380?intlink_from_url=https://www.bbc.com/news/topics/c81zyn0888lt/facebook-cambridge-analytica-scandal&link_location=live-reporting-story

Weng, Q., & McElroy, J. C. (2012). Organizational career growth, affective occupational commitment, and turnover intentions. *Journal of Vocational Behavior, 80*(2), 256–265.

Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology, 59*(4), 662–674.

Yukl, G. (2013). *Leadership in organizations*. Upper Saddle River, NJ: Pearson.

Zagenczyk, T. J., Scott, K. D., Gibney, R., Murrell, A. J., & Thatcher, J. B. (2010). Social influence and perceived organizational support: A social networks analysis. *Organizational Behavior and Human Decision Processes, 111*(2), 127–138.