AFP PHOTO/IGOR STEVANOVIC/SCIENCE PHOTO/IST/SCIENCE PHOTO LIBRARY

Hacking and the darker side of social media

Peter Verhezen

is principal of Verhezen & Associates, a governance and risk consultancy, and a visiting professor at Antwerp Management School and Melbourne Business School.

Peter Chambers

is the chairman of the audit committee of Excelcomindo Axiata, Indonesia's third-largest mobile operator, and a board member and adviser to multiple companies operating in Indonesia.

We analyze the darker side of social media that can easily be exploited in cynical and divisive ways. There is no better example than Russian agents' use of Facebook in the months leading up to America's 2016 presidential election. Today, marketers and for that matter politicians can now design online ads or messages for any target audience, defined at a level of demographic and psychological detail that will boggle your mind.

And with fine-tuned algorithms, Facebook and other social media tools can pick out exactly which users to target who could be receptive to its message. Almost unconsciously, most Facebook users have accepted "data for gossip" in return for their continued use of the platform. Political groups can target certain groups with ruthless algorithmic efficiency to influence their voting behavior. Corporations and institutions, therefore, have the fiduciary duty and responsibility to protect corporate assets and data that could be misused by unaware employees or malicious hackers attempting to access sensitive data or spread “fake news” for cynical political purposes.

Emotions, ‘fake news’ and data security

Indeed, emotions and social media may still incite an upset in the upcoming presidential election in Indonesia. In a time where facts and “fake news” seem to stand next to each other, one should be expected to be ready for about every statistical possibility and not take the incumbent’s current lead for granted. Activists behind the social media campaign #2019GantiPresiden, or #2019ChangePresident, have launched well-organized and well-structured strategies to criticize the administration of President Joko Widodo. They have used religious and economic issues to attack the incumbent president. For example, they have accused President Joko of allowing the persecution of *ulama* (Muslim religious leaders) and discrimination against Muslims, and blamed him for higher prices for staple food items. The rising popularity of the #2019ChangePresident campaign has met with a backlash from President Joko’s supporters and the police. Can this opposition campaign be considered a game changer?

The president’s supporters, local police and the intelligence officials have thwarted recent events to promote #2019GantiPresiden in Pekanbaru, in Sumatra, and Surabaya, in East Java. This has fueled accusations that state security agencies are not being impartial. Such reactions from the president’s camp demonstrate a growing fear that the campaign might prevent him from being re-elected.

Indonesia is battling a wave of “fake news” and hoaxes and online hate speech ahead of the presidential election in April. A string of arrests underscore fears by the government that such data and information-mongering could crack open social and religious fault lines in the world’s largest Muslim-majority country. We already got a brief taste of this alleged religious battle in the Jakarta governor’s election in late 2016 and early 2017, with incumbent Governor Basuki Tjahaja Purnama bearing the brunt of it.

The pluralist nation’s reputation as a bastion of tolerance has been tested in recent months, as conservative groups exploit social media to spread lies and target minorities. Police have cracked down, rounding up members of the Muslim Cyber Army, a cluster of loosely connected groups accused of using Facebook, Instagram and Twitter to attack the government and stoke religious extremism and create social conflict with a “we against them” type of slogan. The group has at least four ideologically driven clusters that spread inflammatory material with the help of bots – software programs that run repetitive tasks – or by hacking into opponents’ online accounts, according to the digital rights group SafeNet.

Some 130 million Indonesians – about half the population – spend an average of nearly three and a half hours a day on social media, one of the highest rates in the world, according to some sources. Many Indonesians may think that every article and video on the Internet is correct or true, because the average Indonesian citizen may be affected more by emotions than by digital literacy, distinguishing potential hoaxes and “fake news" from factual descriptions. Social media and the danger of launching smear campaigns, negative and nasty political campaigning and/or launching reputable "fake news" or "disinformation" circumventing cybersecurity could unfortunately be expected to play an increasingly dominant role in the 2019 elections.

An annual study of Internet freedom globally sounded the alarm bell a few years back, stating that it was observing countries where the regime in power was trying to manipulate social media to influence how their own constituents would think about voting for them. It was only a matter of time before those techniques and tactics would be adopted within their own and, subsequently, other countries. Unfortunately, companies still get hacked far more often than they admit, meaning true transparency may be a long way off. Even Facebook, a major social media player, gets hacked. And turning unwarranted information into social media, whether inaccurate or even fake, seems to be swiftly becoming the "new normal." With a growing young population that is increasingly social media savvy, manipulation of (dis)information may become a destabilizing factor in the upcoming Indonesian elections – especially if you only need to sway between 5 and 15 percent of the (undecided) voters.

Internet and telecommunications companies have learned a few lessons from the 2016 elections in the United States, and we suggest that Indonesian companies, Internet providers and telecommunications companies should be committed to doing their part to ensure malicious actors can't misuse online platforms or services. We believe that social media providers have an obligation to be responsible for their content and work to ensure the legitimacy of their products prior to the forthcoming elections. If, for instance, pornography on social media and the Internet in general is legally forbidden – not to offend pious people within Indonesian borders – one could easily argue that any form of hate speech and deliberate misuse of information should be considered inappropriate as well. Many other countries have adopted such regulations; Indonesia could apply something similar in the name of preserving social order and harmony, as the national philosophy Pancasila prescribes. Admittedly, developing criteria that determine what is hate speech or "fake news" is always culturally and politically contextual, and often affected by powerful (political) lobbying groups that may be partially at the root of the problem.

Anything seems to be allowed in politics: decency is not necessarily on the table.

And since we should be realistic not to expect proper and tougher privacy rules and oversight for political parties at this time, we know that the data they harvest from the electorate could be potentially used for political reasons. And as we have seen before, anything seems to be allowed in politics: decency is not necessarily on the table. If everyone is looking after their own tribe's interests, cultural concerns or religious compatriots, who is looking after the common interest? The current anti-globalization tendency (as seen with Brexit, Donald J Trump's election and inward-looking identity politics in Europe and elsewhere in the world) seems to favor this search for identity at the expense of a moderate form of multiculturalism, harmony and tolerance.

Such as in many other countries, there's a war for talent, especially in big data analytics and data security. Most telecommunications firms and high techs are competing for the same talent. There is a monumental, daunting task ahead to make sure that everything is secure and goes flawlessly during the presidential election on April 17, and that every vote is counted the way it was cast. Empirical data has shown that leading up to last year's Malaysian elections attempted hacks significantly increased and there have been some successful financial ransom incidents. Seeing a similar increase in cyberattacks in Indonesia in recent months, and taking into account Indonesia's immature cyberprotection, it can be safely assumed that malicious hackers are waging a war for financial gain and possibly political gain. We are almost certain that some cyberattacks will result in successful breaches – with unknown consequences.

Weak cybersecurity

In addition to the darker side of social media that can lead to "fake news" and hate speech it is now obvious that the rise of networks and the growth of the "Internet of Things," with its billions of connected devices and software applications, have resulted in a wider array of potential vulnerabilities. Once hackers can get into a network it will cost companies, institutions and/or government agencies a lot of lost time and money, and burn up resources just to remediate the damage done.

Since the dawn of the computer age, malware has been appearing at an alarming rate, and the market began to respond with a large armada of application firewalls and antivirus protections in the early 1990s. The solutions evolved to fight malware in a much more pervasive way are multiplying fast, and so are the daily attacks by hackers.

There's a war for talent, especially in big data analytics and data security.

Today, antivirus vendors are using artificial intelligence and machine learning to analyze all the data coming through any sizeable organization and to "sense" and signal any anomaly. AI can detect what humans are unable to because of the sheer size of the data sets, and this way of detecting data breaches makes up about 77 percent of breaches that have been investigated to date in the Western world. On the threat detection side, AI inherently tries to distinguish real signal from a noise problem. Basically, small changes in network activity may indicate an anomaly that could signal a real attack.

Artificial intelligence – due to its nature to instantly learn the hacker's behavior rather

AFP PHOTO/AFP PHOTO/IGOR STEVANOVIC/SCIENCE PHOTO/IST/SCIENCE PHOTO LIBRARY

than simply responding to historical attack signatures – is more effective than traditional antivirus measurements. Old antivirus software was intentionally programmed to recognize specific security threats, be they viruses, worms or ransom, based on clever heuristics and specific digital signatures, scanning through all the data and files, without any intelligence. New security threats cannot be recognized or known by such antivirus software, which means that these systems need to continuously play cat-and-mouse to catch up with and protect against new threats. And cyberthreats have become more numerous over the years, sometimes becoming too sophisticated for legacy antivirus measurements to keep up. "Teaching" this antivirus software has therefore become redundant. In 2017, experts discovered more than seven million new malware specimens, making that year an *annus horribilis.* To put that figure into perspective, it represents a 5,600 percent increase during the past decade.

Software engineers now fill machine-learning algorithms with millions and millions of examples of cyberthreats, allowing the systems to "learn" how to distinguish benign from malignant cyberthreats. All major corporations should be looking into the artificial intelligence approach that may offer multivector cyberattack prevention. Indonesian companies run huge risks of data being accessed and manipulated at different stages of cyberprotection. There are numerous data banks in big Indonesian companies, and they do not necessarily have a standard level of appropriate protection. These weaknesses have resulted in access to sensitive data by analytic companies and politicians. Every month, telecommunications and other companies have seen millions of attempted breaches from outside hackers, with a considerable increase in recent months.

Within Indonesia alone, one has noted millions of daily attacks and companies have huge difficulties to address, cope with or prevent such cyberattacks. These attempted breaches can be categorized by three main things: (1) trying to financially gain through online ransoms; (2) trying to access financial value to illegally make online purchases; and (3) general hacking for mere pleasure. Other additional reasons could be described as attempted denial of service attacks and general network disruption.

Up until now, many Indonesian firms have focused on improving their respective external protections from outside hackers. However, as we have argued elsewhere (*Strategic Review*, October-December 2018), we strongly believe there is an even higher risk from within the corporate walls. Internal sources – ie, often unconscious but sometimes disgruntled or unhappy employees – may have access to data and be incited to commit a cybercrime for pecuniary or other reasons. Moreover, many Indonesian companies are not even aware of their own digital assets. For instance, through a recent inventory audit, a major Indonesian company identified that 40 percent of the technology assets owned and operated by this company were not even listed or maintained. Such "unawareness" should prompt serious concern because of the significant cyberrisks such sizeable companies are running.

Preventing data breaches and 'fake news'

The Indonesian presidential election will certainly raise the stakes and emotions in the next couple of months. On the one hand, we believe that all the tricks will be used to convince unaware or undecided voters to switch camps. "Fake news," hate speech and hoaxes on social media may not be avoided. Not only will this darker side of social media distort the real story or narrative of the candidates, its manipulation could undermine the process of democracy itself.

There are numerous data banks in big Indonesian companies, and they do not necessarily have a standard level of appropriate protection.

On the other hand, we suggest that Indonesian institutions and organizations that supply and provide data and information should take their duty seriously to protect the integrity of the social networks and data on those networks. And the Indonesian government should be an impartial enforcer of the law and address any potential gross misuse of data and information on social media or elsewhere that could (intentionally) lead to social unrest and disruption. Hate speech should not be tolerated. And finally, organizations and firms (especially those providing networks and data safety on the Internet and mobile networks) should address these cyberrisks. And social media companies especially have a responsibility to prevent such potential data breaches and control where possible the dissemination of sensitive fake news that could result in social unrest.

In the short term, we recommend companies take a couple of actions that could enhance cybersecurity:

First, prevent by focusing on robust digital hygiene. This means that firms need to stay updated with the current and latest technological advances. It also implies that firms follow rigorous backup practices and adapt similar procedures as in the case of disaster recovery, where the backup data resides on a different network and database. Organizations should ensure that appropriate patch management is implemented and that the latest patches have been identified. Organizations should identify the key risks for each of the networks and data banks within the firm and to focus the security improvement activities on those identified sensitive areas.

Second, prevent cyberbreaches by having implemented a thoughtful design of IT architecture. Important intellectual property, customer-related proprietary information or sensitive strategic information should be protected in a special database separated from the other organizational databases. Proper authentication and security controls, such as introducing two-factor authentication as in a password in combination with biometrics or tokens, should be implemented. Indeed, any firm should understand the different assets within the company and its network and to understand where the sensitive data is kept and stored. Any organization should make efforts to improve the internal controls over access management and user identification, and ensure that the access of former employees is deleted. Clear protocols for external partners that can and use access data within the company should be established. And finally, having strict management protocol and standard operating procedures in place on the use of external and third-party devices within the firm's network is a must.

Third, prevent cyberbreaches by enhancing the ability within the firm to detect intrusive behavior. As we argued before, human error is still the most prevalent means of gaining access to proprietary and sensitive information. Effective risk management practices rarely allow sensitive information to be released to third parties or any outsider inadvertently. Proper procedures to access data in the organization should be in place. We also strongly suggest to either install an internal unique security operating center or subscribe to a third-party service to monitor in real time any attempted breaches.

Fourth, for possible cyberattacks through advance planning and rehearsal, in the same way as one prepares for floods, tsunamis or fire, one should have a clear execution plan on how the organization will respond if there is an attack, and who will be accountable for which aspect. And one needs to organize and rehearse the expected responses in case of an actual cyberattack. To ensure an appropriate response in case of a cyberattack, all cybersecurity activities should be managed and supervised under a unique senior-level position with a direct reporting line to the supervisory board. And a word of caution in the event of a data breach where financial ransom occurs, we recommend not to agree to these demands and to push back and take a non-negotiable position (where possible).

And fifth, embrace the possible adoption of cloud technology to reduce cyberattacks. The big advantage of cloud technology is that these systems are updated and the providers have engaged with artificial intelligence and machine learning to accumulate data in real time about cyberattacks and intrusions, which allows these advanced IT companies to incorporate built-in constraints through different layers.

In other words, organizations and institutions in Indonesia and globally should become more resilient against possible cyberattacks, prevent such potential cyberbreaches as much as possible, and in case they do occur, be well prepared to take action and address the attack. Indonesian security and information and computer technology agencies have a big job ahead of them, and so do social media-related companies, in rooting out fake personas and misinformation campaigns. The focus should be on securing proper procedures and information channels in companies that underpin the distribution of data and information through social media, and in companies and their websites that provide relevant information, avoiding hate speech and minimizing “fake news” that could hurt social order and harmony within Indonesian society.