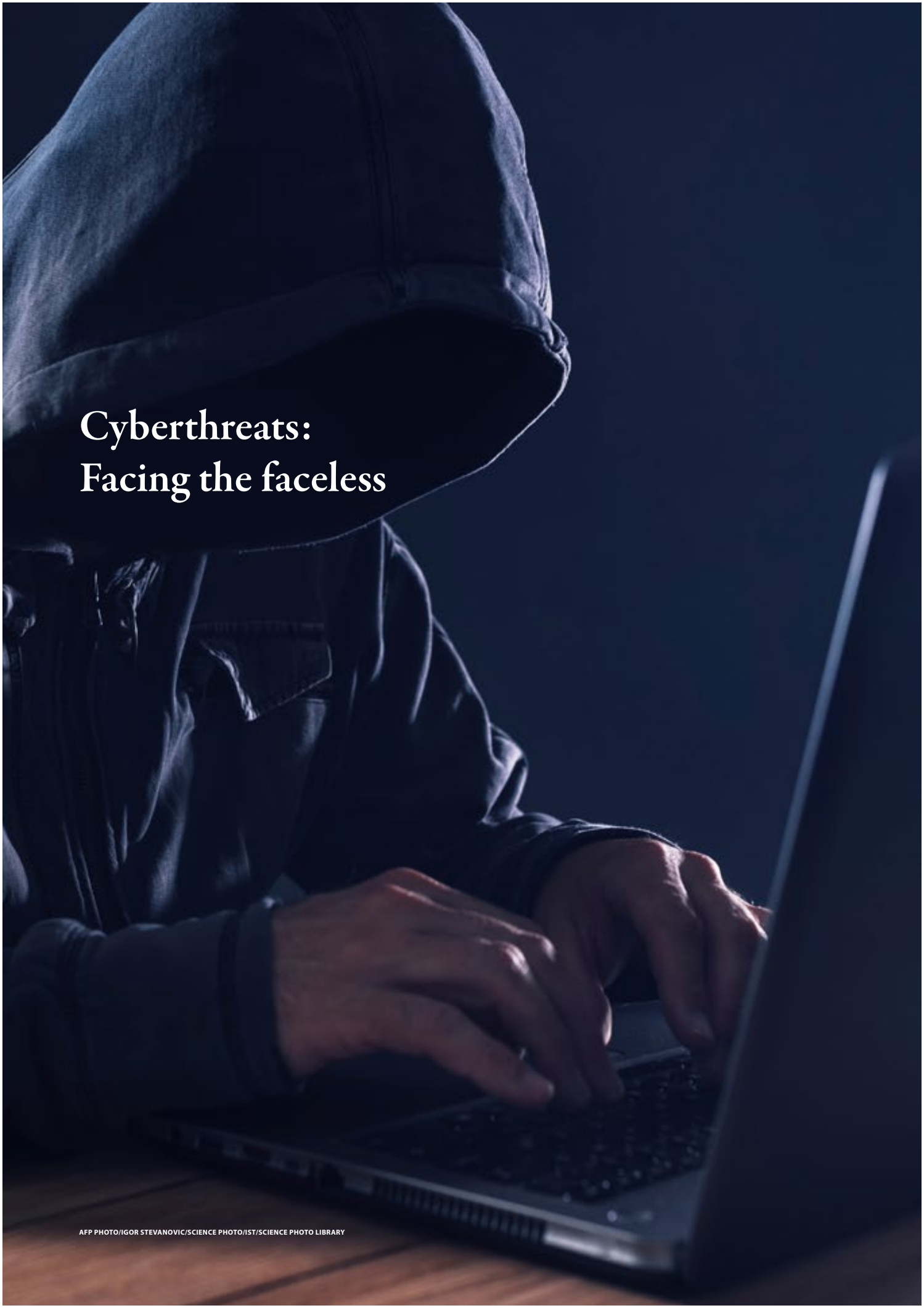
Cyberthreats: Facing the faceless



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

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

Steven De Haes
is a full professor in information systems management at the University of Antwerp and the incoming dean at the Antwerp Management School.

During Malaysia's recent general election, there was an uptick in attempts to hack into Malaysian telecommunications companies, in an attempt to influence the election outcome. We can expect a similar increase in attempts to hack into Indonesian telecommunication firms and other sensitive organizations during the upcoming elections, in April 2019.

One of the mistakes company boards often make about cybersecurity threats is to see the risk as merely "IT-related" rather than a business risk. Indeed, companies increasingly face new exposure and the operating environment becomes more digitally connected by the day. Because of this digitization, organizations have also become more vulnerable to potential attacks on their data and networks. Cyberthreats ranked fourth on the list of perceived threats among chief executive officers in 2018, up from tenth a year earlier, according to a 2018 survey of CEOs by PricewaterhouseCoopers. Similarly, a 2018 McKinsey & Company study found that despite the acknowledged priority of cybersecurity, only 16 percent of experts considered their companies to be well prepared to deal with cyberrisks. And this lack of preparedness extends not just to private companies, but also to governmental institutions and, to a lesser extent, nongovernmental organizations.

What are the possible risk scenarios? About three-quarters of international global board members of private organizations believe that their companies would respond effectively in a crisis; yet fewer than half of these companies have taken steps to be truly "crisis-ready." Incidents and fallout from cyberattacks vary, including critical data loss; business interruptions and customers lost; property damage; theft; adverse media coverage; regulatory actions; profits impeached; loss of trade secrets or confidential information; extortion; breach of contract; product recall; network security liability and other liabilities.

We believe risks that pose a potential threat, especially those related to the security of our data and networks, can no longer be ignored. Any business executive should be prepared to take measures to prevent, prepare for or respond to a cyberattack. Cybersecurity has now become a major threat to businesses. Indonesia and Asia in general are no exception. How do we interpret this specific cyberrisk? Once we have a better understanding of the nature of this risk, organizations can address it more effectively.

An integrated perspective

What are the causes of particular risks and their potential unfolding crises? Risks can be interpreted as either operational, strategic or external in nature, according to Harvard professors Robert S Kaplan and Anette Mikes. Operational or preventable risks arise from within the organization and are usually controllable, and should be eliminated or avoided because companies do not strategically benefit from taking them on.

Examples include the risks associated from the unauthorized, illegal or incorrect and inappropriate actions and risks from breakdowns (as a result of cyberthreats) in routine operational processes by employees or managers. Operational risks should be strictly monitored through proper policies, processes and procedures that guide people's behavior and decisions toward the desired norms. Compliance with standard operating procedures is essential in reducing or avoiding altogether those preventable operational risks.

Strategic risks, however, are risks that the company voluntary accepts in order to generate superior returns from its strategy. Strategic risks are inherent in the business the company is undertaking, but in attempting to achieve such returns the company is required to take significant risks to capture those potential gains. British Petroleum accepted high risks drilling below the surface of the Gulf of Mexico because of the potential high value of the oil and gas it hoped to extract. Software and information communication technology companies such as Google, Facebook and Microsoft reward hackers who find bugs in their software or operating systems, allowing those firms to "debug" these weak links and make them more secure. Moreover, some risks are not just accepted but even sought after, as they could be inherent to innovative processes of trial and error. Executives therefore need to design a risk management system that reduces the probability that the assumed negative risks actually materialize, and where possible optimizes opportunities by taking informed (positive) risks. Innovation always implies a form of (positive) risk taking. Dialogue rather than a rules-based control model is recommended for these kinds of risks.

Finally, uncontrollable or external-related risks arise from events outside the organization and are usually beyond the control of the firm. Examples include policy shifts or macroeconomic crises that affect the organization. And although external risks are beyond the control of organizations, they should be identified, assessed for their potential impact, and risk managers should figure out how best to mitigate their effects should they (improbably) occur, or how to insure against such exogenous threats. Moreover, executives and managers should be aware of the potential cognitive biases that discourage them from thinking and discussing those external risks until it may be too late.

Scenario building or war gaming could be an appropriate way to address these uncontrollable external-related risks. Indeed, multiple research has found that people overestimate their ability to influence events that are actually heavily determined by randomness: we tend to be overconfident about the accuracy of our risk assessments and forecasts, endangering

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

the organization. So yes, organizational and individual biases inhibit our ability to discuss risks and potential failures. We all have seen how groups facing uncertain conditions engage in gathering support within the group and fall in line with an overbearing or overconfident executive, sometimes resulting in disastrous groupthink.

Rather than mitigating the risk, organizations actually incubate risk through the normalization of deviance by tolerating apparently minor defects or deviations instead of being alerted to imminent danger. Accepting such normalized deviance, often driven by overzealous profit or revenue objectives, can backfire and cause unnecessary risks, as the Toyota Camry acceleration debacle in the United States some years ago showed. The danger of risk can be expressed as the combination of the impact, likelihood and resources needed to repair the potential or possible occurrence of the threat.

Although cybersecurity is often interpreted as a threat coming from external sources, we believe that the risk taxonomy allows us to assess these cyberrisks as most often operational-related and thus preventable. Only in specific circumstances may an organization fall prey to an "external" or exogenous cybersecurity risk, when the organization does not and could not have any control over the security breach. In 2010, the Stuxnet worm propagated across the Internet and other networks and caused physical damage and

disruption. This cybersecurity breach appeared to have been targeted at power utilities to conduct extortion, affecting a number of nonrelated industries in the process, for which this utility fallout can be considered "exogenous." In other words, executives and managers should take a completely different approach to those cyberthreats as internally preventable through procedures, processes and compliance programs, and yes, indeed, at least prepare for unlikely – not "foreseeable" – but highly impactful exogenous "uncontrollable" cyberattacks.

The cost of cyberattacks has now eclipsed $400 billion a year, larger than the gross domestic product of about 160 countries.

Risk management, in contrast to management of operations strategy, focuses on negative threats and failures, rather than opportunities and successes. However, most successful companies have arguably well-established and properly functioning risk departments. Moreover, the best risk managers are the CEOs who consider risk as integral to their business, thereby optimizing positive "risky" opportunities and minimizing threatening negative risks.

During the 2008 global financial crisis, Goldman Sachs and JPMorgan Chase, and to a lesser extent Morgan Stanley, weathered the storm slightly better because they had strong internal risk management functions and savvy leadership that understood and managed the companies' exposure to multiple risks. Similarly, in today's context where data and networks are increasingly linked, companies are prone to "unwanted invasions" if not properly prepared. Organizations need to institutionalize risk processes and procedures for each of the different risk categories, as well as processes to neutralize the managerial biases and overconfidence. Better to be prepared than to be sorry. An organization's ability to weather storms depends on how seriously executives and boards take cyberrisk management when the sun is shining and no clouds are on the horizon.

Cyberattacks and cyberfraud have aggravated the ubiquity of Internet-related products and processes. No company escapes the demand for more cybersecurity. However, the good news is that most cyberbreaches can be "internally" prevented. The infrastructure of a digitized economy – the Internet – is characterized by an innovative but very open architecture. It's successful but also contains a fundamental weakness: vulnerability to hacks. ATMs never get hacked because they are a proprietary network. Admittedly, about 80 percent of cybersecurity issues that have occurred in the commercial world are related to internal processes and people, which we label "internal threats." It is perhaps ironic that one of the earliest purposes of the Internet was to create a decentralized, distributed

communications network that could survive a nuclear attack. Because of the ongoing and increasing digitization of production processes within companies, and the growing and increased relevance of the Internet of Things (IoT) and big data analytics, the Internet and intranet have become the preferred and most effective network channel to achieve productivity growth.

The same distributed Internet structure has now led to a whole new class of possible attacks. Whether motivated by politics or profits or mere mayhem, the costs of cyberattacks has now eclipsed $400 billion a year, larger than the gross domestic product of about 160 countries. As the costs of cyberattacks have dramatically risen, so has the industry devoted to countering the threat. Between 2000 and 2020, the cybersecurity market will have grown from $3.5 billion, employing a few thousand people working in IT departments, to $175 billion, providing critical infrastructure to just about every kind of business.

Cybersecurity is really about securing the various networks, thus guaranteeing the reliability and privacy of digitized information that is used throughout businesses. First, the network's confidentiality or information availability could be under attack. A confidentiality breach refers to attacks that compromise confidentiality, aiming to steal or release secure information such as credit card or social security numbers from a given system in an illicit or unauthorized manner. An example is to insert malware – malicious software – in a system, allowing hackers to log into the system and steal private information.

Second, a network's availability or right access to information could be violated. A breach on the network availability – denial of service (DoS) or distributed denial of service (DDoS) – brings down a network by flooding it with a massive number of requests that render the site inoperable. DDoS are exactly the same except the attacked has mobilized several systems for the attacks. DDoS attacks aim to use so many attackers (potentially hundreds of thousands) that it becomes nearly impossible to distinguish the attackers' traffic from legitimate traffic, known as botnet. The targets of botnet attacks are usually big corporations or governments. The 2013 DDos attack on the Dutch ING Bank was such an example, reducing the shareholder value and leading to a flurry of criticism via social media negatively influencing the trust of customers in their bank. ING, not properly prepared for such a network intrusion in 2013, initially denied the attack and evaded questions, which aggravated the crisis.

Third, the network's integrity or integrity of information, as well as the trustworthiness of information, could be breached by illegitimate hackers or intruders. An integrity breach refers to cyberattacks aiming to affect the network's integrity that are more physical in nature. They alter or destroy computer code and their aim is normally to cause damage to hardware, infrastructure or real-world systems. Once an integrity attack has taken over a machine, the machine ends up being rendered useless and is added to the waste stream.

Finally, the authenticity refers to the assurance that an entity claiming an identity does possess the right to use it.

Business transactions as well as information exchanges between enterprise locations or exchanges between business partners or third parties should be able to be trusted (for their authenticity and nonrepudiation). Assigning and authenticating identities will be challenging for the Internet of Things; breaches can be expected to occur. Maybe, "automated" authentication processes enabled by the new blockchain technology would be better. Blockchain can be defined as an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value, according to Don Tapscott and Alex Tapscott, authors of "Blockchain Revolution" (2016), and may be one of the potential solutions.

Cyber exposure versus cyberrisk

Any of the four types of cyberbreaches described above can be considered from two major perspectives, which function as the foundation for integrated [cyber] risk management: (1) a technological or external/exogenous view; and (2) a human-organizational or internal perspective. The technological upgrades as in a unified ICT architecture and state-of-the-art technology are definitely important factors in improving cybersecurity.

However, based on our combined professional experience and expertise of more than six decades in telecommunications, banking and financial services, and the ICT and IT infrastructure sector, and our knowledge as well as academic research in numerous industries and boards, we emphasize the even more crucial need to minimize human and organizational error and improve strategic foresight. Technically, an organization can improve its cybersecurity by encrypting data, using strong passwords, white-listing organizational applications, segmenting the IT environment and patching vulnerabilities. Our experience tells us that it is critical to understand the current asset infrastructure so as to understand what needs to be protected.

And yes, patch management – a strategy for managing patches or upgrades of software applications and technology – is necessary to handle rapid changes in our current VUCA (volatile, uncertain, complex and ambiguous) context. A firm may adopt Cobit (control objectives for information and related technologies) or apply ISO 27000 standards across the firm – or any standard of good practice for information security. Stress testing could be part of enhancing the technology solution. It is often assumed that having state-of-the-art technology solves most problems; that is only half true. In a majority of illicit penetrations into the networks of companies, people have been the weak link because of a weak ethos or weak culture. In other words, humans rather than technology are the main culprits for cybersecurity breaches.

Firms would get rid of at least half of their security problems if they trained their employees and put consistent controls in place. Accountability of the system should be related to monitoring and control, to proper process training, and to regularly auditing people. Strengthening the hardware, software and network procedures may be

AFP PHOTO/TEK IMAGE/SCIENCE PHOTO/ABO/SCIENCE PHOTO LIBRARY

important, but addressing the managerial, organizational, people and strategic aspects is even more crucial. The unauthorized disclosure of personal data and system outage events is another key element that contributes to cyberrisk. The flow of data and information from internal points to points external to the company can be quite substantial and part of a business model. However, such flow from an individual employee to an external partner may implicate potential threats that could be viewed as malicious, especially if the user is relying on personal Yahoo or Gmail accounts.

Ironically, these personal communication tools – they cannot be monitored or controlled by the organization – that could be an attempt to evade this internal control can sometimes be a blessing when malicious external parties use these non-organizational emails to intrude in personal data. Since they are not directly linked to the organization, it limits the damage to the organization. In particular, losses deriving from the unauthorized disclosure of personal data have a higher severity and frequency than most other risks. A recent high-profile example of this type of loss is the case of the large US retailer Target, which suffered a breach involving approximately 40 million payment card records and the personal data of around 70 million further individuals, following the infiltration of its corporate network via a link with a third-party contractor. The breach resulted in significant costs incurred to respond to the incident, in

addition to defending liability claims. Mistakes by network administrators and users can easily open the door to the overwhelming majority of successful cyberattacks. And unfortunately, quite often the danger of a cyberattack originates from within the walls of the company, be it an employee or vendor. Media attention has recently focused on data privacy violations where Facebook's reputation took a hit when it was revealed that the private data of 80 million Facebook users was unknowingly sold and used by external parties. However, the attacks involving connected companies or direct employees statistically pose a much graver threat since these insiders have much easier access to systems and incite much greater windows of opportunity for hackers. Every organization should establish clear policies and procedures to address any form of sensitive communication or data flow that is prone to cyberthreats.

It is estimated that between 50 percent and 80 percent of all cyberattacks are aided or made possible by insiders, most often unintentionally – typically through some kind of targeted "phishing" expedition that involves emails containing a link or attachment to click on. Indeed, phishing scams are still the root cause of most data breaches, where employees are fooled by plausible emails into opening malware-laden documents that infect their computer and subsequently the whole network. Or employees are conned by email scams. So training employees to become cyberaware is crucial in the fight to strengthen cybersecurity. And finally, it is virtual impossible to be immune to cyberattacks. Only when the corporate culture makes cybersecurity the responsibility of everyone can a lot of the primary culprits of network security breaches be addressed. Companies need to develop and maintain a safety culture and a mind-set to continuously improve cybersecurity. One can build strong doors to protect the place, but when we leave keys lying around, it will not get safer.

Hence why a number of human or organizational barriers to greater cybersecurity can be distinguished and should be mentioned. We think of inadequate management and organization processes, for instance, which are often undermined by a lack of management commitment or priority, and without a clear strategy with respect to cybersecurity. In addition, too many angles lead to confusion and consequently to misguided perceptions or attitudes that function as barriers (instead of decreasing cyberthreats), and the unhealthy belief in information security is a mere technology issue, which again leads to the

Indonesia and most of Asia's cyber exposure is surprisingly less than Finland, which is one the most cyber-savvy and connected countries in the world, and thus a good benchmark.

denial of the cyberchallenges or security holes that no one is willing to admit. And inadequate levels of skill and knowledge obviously result in a lack of insight to secure data and networks, unintentionally resulting in too much reliance on the IT department. Finally, a lack of sufficient or dedicated budget, whereby security is seen as a cost instead of an investment, where no returns are seen. How to deal with these barriers that aggravate cyberrisks?

The insider or people-related organizational threats are often unappreciated, while detecting and preventing insider attacks has become much more difficult. The reasons for these increased cyberattacks are likely due to the fact that there has been a dramatic increase in the size and complexity of IT, plus employees increasingly use personal devices for work. No doubt, the explosion of social media has also enhanced the vulnerability of those [inside] users.

Interestingly, Indonesia and other Asian countries currently do not fare too bad in terms of vulnerability to possible cyberattacks, according to researchers in Singapore. This cyber exposure is measured by the degree of disclosure of sensitive information (such as company valuations and trade secrets), exposure of credentials to non-legitimate intruders and targeting by hacker groups. Mikko S Niemelä, from Kinkayo, a Singapore cyberintelligence firm, measured that Indonesia and most of Asia's cyber exposure is surprisingly less than Finland, which is one the most cyber-savvy and connected countries in the world, and thus a good benchmark.

Counterintuitively, the most exposed countries to global hackers, according to this study, are advanced European economies because these digitally more mature European organizations have been compromised to a greater extent than Asian organizations that often still store valuable data in a very physical way. The more advanced Western firms store data on the cloud, giving cybercriminals an incentive to come after them. Nevertheless, Asian firms are catching up fast, closing the digital gap and thus their potential exposure to cyberattacks. However, according to Niemelä, Asian firms have an advantage of late-stage entry compared to these more vulnerable European companies that are burdened by more ineffective and cyber-vulnerable software and hardware infrastructure.

Asian companies have often bought off-the-shelf enterprise solutions and reliable communication platforms, and Indonesian employees often use personal emails that are not directly linked to workplace servers, which are potentially very vulnerable to attacks. A temporary advantage of being currently slightly less cyber exposed – likely because "only" 30 million of Indonesia's 260 million habitants use online commerce, worth about $5 billion in revenue in 2017 and likely to grow exponentially in the coming five years – does not mean that Indonesian companies should become complacent. And one should not forget that 99 percent of all transactions by volume in Indonesia today are cash-based. That could change fast, though.

However, according to a McKinsey report released in August, online fraud in Indonesia is among the highest among Asean countries, ranked number 70 out of 165 countries in

terms of cybersecurity – a clear disincentive for consumers and merchants who might pursue online commerce. Moreover, online orders originating in Indonesia are 12 times more likely than the global average to be fraudulent. Among Asian countries, Indonesia is not faring very well at all in terms of vulnerability to malware threats and network attacks. Only Vietnam, Laos and Myanmar are doing worse in Asia, according to the McKinsey study.

China's (as is Russia's) ability to affect the Internet is well documented and understood in geopolitical and policy-making circles. And let us not forget that the telecommunications industry, information technology services and financial services – true for both Western as well as Asian countries – are the most exposed to cyberattacks, much more than utilities, energy and real estate industries that are slightly less prone to cyberrisks. The fact that we have seen more attempts to attack Malaysian and likely soon Indonesian telecommunications companies suggests that Asia will become increasingly more exposed to malicious cyberattacks.

The role of management and boards

The consequences of a potential cybercrime or cyberfraud are not limited to a one-time financial hit, but also involve reputational damage, in-depth regulatory investigations, long and costly litigation, and obviously the theft of intellectual property. Companies urgently need to prepare for an appropriate integrated risk management defensive system that aims to prevent such cyberthreats, and if necessary assess, detect and respond to cyberattacks. All organizations benefit from an integrated and comprehensive approach to risk management, security and control. As organizations take advantage of the opportunities available through global networks, and comply with existing and new security laws and regulations, difficult decisions increasingly arise about how much money and where to invest in IT security and control, and all this hopefully in a "sustainable" and profitable manner.

A defensive cyber-program

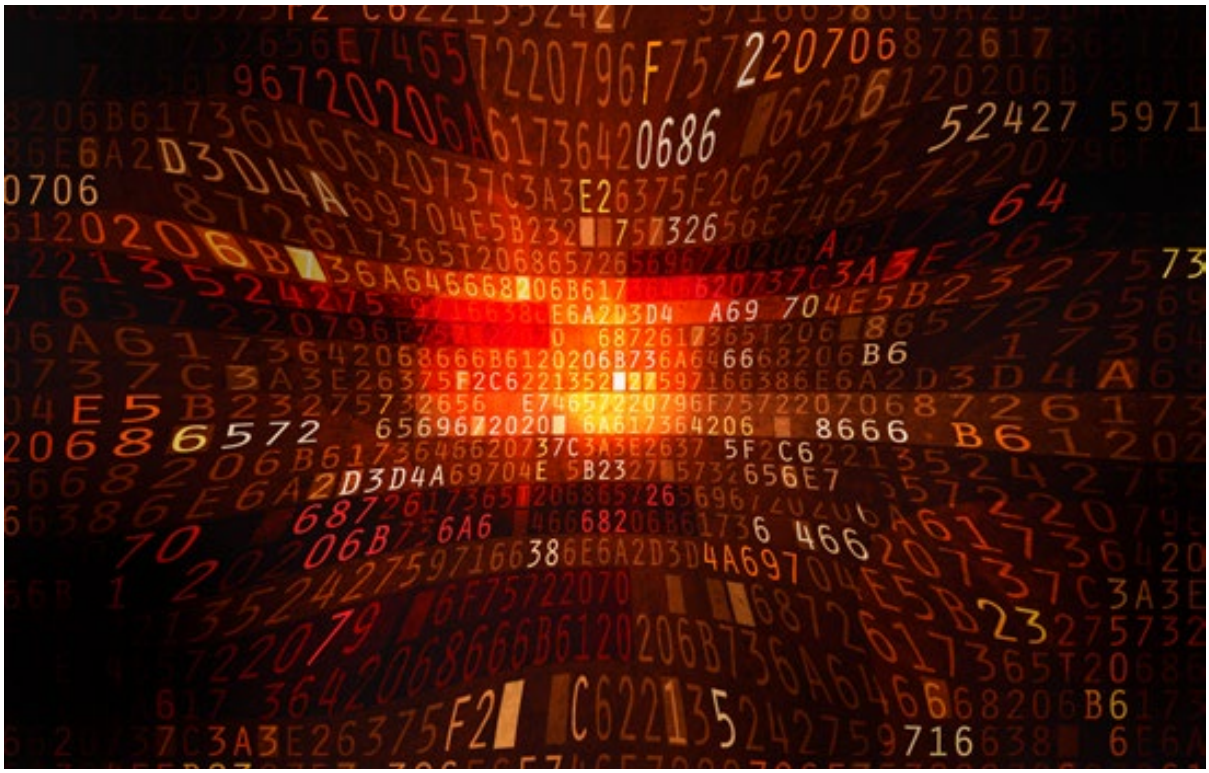
Often, board directors unfairly blame IT for cybersecurity failures that actually originate from technological or external sources such as vendors. Exposure in cyberspace is defined by how connected your organization is and what its dependencies are. The more the organization relies on third-party services, the more vulnerable it becomes. Cyber-exposure as a result of this dependency means that the company's assets and services, as well as organizational or internal processes, are somehow accessible through public networks. Such exposure points include technical assets such as networks; systems and online applications; people (email, social media and mobile); information flows between systems; processes (maintenance, software development, banking transactions); and current security measures for each technical asset.

As argued above, people close to the data or other corporate assets can often be a weak link in a company's cybersecurity program, especially when they share passwords or files over unprotected networks or click

on malicious hyperlinks. Organizations are often unable to identify essential interventions and struggle because of insufficient knowledge and skills, while this absence of implementation of core information and communications technology (ICT) interventions could endanger the cybersecurity in those organizations. This is why communication between business and cybersecurity seems to be often misaligned. In other words, nonalignment between management and organization, as well as misperceived perceptions and attitudes vis-à-vis cybersecurity, should be addressed, while training and educating personnel on being aware of cyberthreats is crucial in enhancing cybersecurity. Tragically, the Achilles' heel of organizations is also the lack of ICT understanding and advanced knowledge about cybersecurity by both top executives and board members.

Effective practices, therefore, need to be implemented from the top-down and from the bottom-up to ensure that the monitoring systems are always up to date and that everyone remains vigilant for suspicious activity in the systems logs. The organization needs to have a coherent plan to deal with cyberattacks. First of all, senior management needs to be on board. Sustained support from senior management is crucial to ensure that action plans are in place to mitigate the risk of cyberattacks or cyberfraud. No matter how technically savvy managers or competent IT executives are, mitigating risk remains everyone's responsibility, and such a message can only come from the top. Board and executive leadership benefit from establishing a cybersecurity committee to oversee the security and risk programs in the organization, whose chief information security officer directly reports to the CEO, implicitly endorsing the importance of such an oversight committee. And it goes without saying that accountability for the risk and security management of sensitive and strategic data and information is to be separated from the ownership management of these data and information assets. In addition to the audit function of the committee, we also suggest management design and install a security operating center that gives executives and management effective real-time monitoring of the network – both for internal and external threats.

Second, the organization needs a proper security strategy. Good technology is necessary but definitely not enough. Besides the technological aspect, focus should be given to the human aspect of cybersecurity because this is often the weakest link. This is why cybersecurity should be looked at from an inside-out perspective to understand what employees, strategic business partners and third-party vendors are doing within the organization, and how they interact with high-value assets such as systems, facilities and data. In addition, the organization should also emphasize an outside-in view to consider what a potential attacker or hacker might see when scoping out weaknesses from the outside. Such "turning the map around" may allow corporations to prepare for actions an attacker may undertake in the future. In developing such coherent cyberstrategies, organizations need to make choices: do they build full-fledged in-house security capabilities, or do they want



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

to rely on external experts or consultants, or do they prefer to adopt a hybrid approach? It is recommended that organizations focus on their core competencies while taking advantage of the skill set of their in-house IT and information security experts.

Third, an organization needs to build security awareness through effective awareness training. Management should encourage behavior and processes that guarantee that information security is integrated within daily routines. Salesforce.com, for instance, voted the most innovate company in 2017, has applied a gamification program – an online exercise in the form of a game as organizations have established for ethics programs – to help make employees much less likely to click on a phishing link and instead report it to management.

Fourth, organizations need to create alliances where IT security staff can coordinate and share information within their organization, but also within the industry and even with their competitors. Sometimes, organizations cooperate with government agencies to reduce potential successful cyberattacks. We recommend not just collaboration within the organization and between organizations, but also between private organizations and public institutions to reduce cyberrisks.

Finally, organizations should follow and apply best practices. Security policies are only effective when organizations have a rigorous and continuous manner of monitoring compliance. Confronting cybersecurity threats

implies keeping defensive processes up to date, continually training personnel, staying currently informed on the latest state of information security and using control-enabled tools to proactively detect, analyze and respond to breaches in the network or IT security.

In essence, three lines of defense should be brought in or strengthened to enhance cybersecurity within the organization. The first line of defense is the usual proper management control mechanisms and internal control measures, as has been historically developed to guarantee financial (accounting) integrity. These internal control measures vary from process controls such as encryption, antimalware and data leakage prevention to organizational policies (as segregation of duties) and standards that make everyone in the organization responsible for the network and infrastructure. The second line of defense is the crucial reliance on a proper and effective information office with a skillful chief information security officer who is responsible for the appropriate monitoring, reporting and tracking of key controls to be performed by the IT operations, be it risk management, financial control, quality management or compliance. This second line of defense also implies proper IT governance (which we'll explore a bit later). Finally, the third line of defense is an internal audit which reviews the first and second line to ensure the controls are effective, have suitable coverage and are proofed with evidence so the external auditor and regulator can perform their respective external duties.

A safety culture usually implies management applies a three-pronged approach within each of these three lines of defense: prevention, discovery and recovery. Admittedly, most organizations – with the exception of financial services that are doing a better job on average – are poor at prevention, pretty weak on detection and most probably terrible at recovery. Emphasizing the technological or IT aspect without focusing on the people will increase the risk of a cyberattack on your organization by at least 50 percent. Cybersecurity is not solely the IT department's responsibility. It has become everyone's responsibility and certainly the board's responsibility.

The essence of preventing cyberattacks is to understand the business risk of the company, especially to strengthen the network weaknesses. Once the business risk has been clearly expressed and figured out, the organization can translate and understand the technical implications better and more effectively. This means that it all starts by assessing and knowing what and where the high-value or crown jewel assets of the organization are, what connects those assets and how someone would access them. If management understands the environment and the platform where its crown jewels reside, it will allow management to control and thus protect this specific environment better. One closes a complex environment down to simply the environment, just like the United States Secret Service does if the president is to address an audience in an auditorium. Creating firm boundaries for your data center to better control and protect the organization's crown jewels will actually also make detection and response easier. Implicitly, by prioritizing

alerts, organizations will be doing a better job in exerting control over their data. In addition, increased oversight in a particular open ecosystem needs to be structured in such a way that it does not slow potential innovation.

In order to prevent cyberattacks, cryptographic signatures should be used to check the integrity and authenticity of firmware (interface between hardware and software). In addition, there should be some kind of specific authentication process (identification and password). When firmware is stored on a read-only memory, malicious changes to the firmware become impossible. And firms should regularly use firmware analysis tools that allows them to rate the current security level of the firm's system. In the case of a successful cyberattack, companies should be able to detect exactly how it occurred and defend against future attacks. To do so, malware scanners – similar to antivirus solutions for personal computers – scan firmware updates or the firmware itself looking for known malware. Moreover, intrusion detection systems can also look out for malicious behavior, either in the network traffic or in the device itself. And finally, integrity-checking concerns detecting changes to firmware while it is running on a device.

And just as important as preventing and detecting a cyberattack is how a company responds to it. The first order of urgency is to clean up the attacked systems and restore them to normal operations. But a thorough investigation should also follow. An incident response team should be in place in case a crisis hits the company. Moreover, the incident response team will need the IT forensic tools to analyze network traffic, hard drives, memory and so on. Finally, the team will need specific tools for analyzing malware and other forms of attack.

Properly responding will require a crisis-ready leadership. The best defensive system is to prevent the risk from occurring and to be ready to address the threat in any case and under all circumstances. In other words, organizations would be better protected with a crisis-ready leadership team. We believe that top leadership will need to implement good governance and accountability to anyone in the organization. And on top of these governance foundations, leadership should design, install and implement an effective response system.

Any organization should be prepared to handle a potential cybersecurity breach that may result in an "abnormal and unstable situation that threatens an organization's strategic objectives, reputation or viability." In preparing leadership for such crisis situations, one should (1) challenge the optimism bias of decision-makers, (2) cultivate a crisis-ready culture and (3) prepare the organization to respond.

For Indonesia, the country needs more innovation to help the ecosystem grow to sufficient maturity so it can become competitive to prevent global players entering and dominating the local market.

Conclusion: Savvy boards

In our increasingly digitized economy, information technology and cybersecurity have become fundamental to support, sustain and grow organizations. Successful

And just as important as preventing and detecting a cyberattack is how a company responds to it.

organizations leverage the digital innovation potential, but also understand and manage the risks and constraints of technology. Emerging research and practical experience at technology-oriented firms call for more board-level engagement in the enterprise governance of IT, its cybersecurity and identifying serious consequences for digitized organizations in case the board is not involved. We believe that cyberthreats do not just derive from poor information and communication technology – the external perspective – but more often than not are caused by internal human errors and organizational weaknesses.

This essay provides guidance on the what, why and how boards can take up their accountability in governing the digital assets and how to improve cybersecurity. Although Indonesian companies and most other Asian corporations may be less digitally connected than their Western peers, making them slightly less exposed to cyberattacks, complacency would be misguided. Indeed, the digital gap is in the process of being swiftly bridged, and soon those Asian companies will be as digitally exposed as anyone else. An integrated risk-management approach goes beyond compliance and prepares for eventual cyberattacks through scenario building, war gaming and reducing blind spots. It also emphasizes both the human, organizational and technological sides to prevent or prepare for cyberbreaches.

The typical time between cyber-penetration and its detection is 205 days, according to some experts. Not if, but when, is the adage here, taking the warning of experts such as John Chambers, former executive chairman and CEO of Cisco, who famously quipped: "There are two types of companies: those who have been hacked, and those who don't yet know they have been hacked."

Every organization will need a clear roadmap to test the system and procedures for a crisis, and should comply with the best standards and regulations, such as the recent European General Data Protection Regulation. By developing digital tools, facilitating and monitoring board members could gradually engage in decision-making and control of digital assets, and become more cyberfraud resilient, which implies better monitoring and control of cybersecurity at the board level. Resilience starts with the board, which should oversee and adopt an effective risk management system – which also assumes the board appoints a member with specialist technology or cybersecurity experience, able to understand the vulnerability of the company and guide it toward better security and data protection. Bigger companies can internally enhance their cybersecurity ability, whereas smaller companies may need to seek third-party expertise to initially assist. By having better processes and procedures in place to prevent cyberattacks, the organization will also better

detect and react to possible breaches. We argue that the use of a kind of cyberrisk dashboard could be very instructive and helpful for boards and even executive leadership. However, the board should also have prepared a clear post-breach plan of action in case of a cyberattack and data breach, which under international regulations will need to be disclosed (not necessarily under Indonesian rules yet).

Installing more accountability and transparency within the organization will allow organizations to be better prepared to prevent and thus to detect and react to cyberfraud. This, consequently, will increase stakeholder trust in the organization's ability to address cybersecurity more effectively. Investors want to know who on the board is responsible for cybersecurity and, when the attack occurs, to determine the damage and assure appropriate arrangements are in place. Institutional investors are increasingly looking for more engagement with the audit committee chair over cyberrisk concerns. Such an intangible asset of trust will allow the organization to gain some competitive advantage and potentially reduce cyberattacks. The current complex and uncertain environment of organized cybercrime, malicious software and dark web activity means that boards will need to raise the bar to protect their crown jewel assets and the personal data of the company and their clients, and to address all of the concerns of stakeholders.

And although Asian, and in particular Indonesian, organizations may have their data and information slightly less fully stored in the cloud, network and data security will also play an increasingly important role in their operations. Hence why any board and top executive should be prepared for cyberthreats and prevent them occurring through both technological as well as organizational solutions. Hoping that you won't be hit by a cybercrisis waiting to happen is no option at all. Better to be prepared than sorry, especially if you have a fiduciary duty of care, prudence and loyalty to your organization.