McKinsey&Company

Cybersecurity and digital resilience: Seven practices for companies in Indonesia

A robust cybersecurity program requires much more than increasing spending on security risks—digital resilience must also be built into business processes and systems.

Vishal Agarwal, Aman Dhingra, and Michael Gryseels

SEPTEMBER 2018 • INDONESIA OFFICE

© gorodenkoff/Getty Images

The Indonesia Security Incident Response Team on Internet Infrastructure reported 205 million cyberattacks in 2017. Cyberattacks can be costly, and their scope is widening. Until recently, financial companies and governments were the primary targets of cybercrime. No more. The NotPetya and WannaCry ransomware attacks of 2017 affected companies in a wide range of industries, including several institutions in Indonesia. Furthermore, the discovery of the Meltdown and Spectre flaws on computer chips showed that cyberrisks occur not just in software but also in hardware.

Many companies, in Indonesia and elsewhere, will need to do much more to protect themselves from cyberrisks. In a recent global survey, 75 percent of executives said they consider cybersecurity a top priority, yet only 16 percent said their companies are well prepared to withstand cyberrisks. Merely spending more is unlikely to help. Our research on 45 Fortune 500 companies found no direct correlation between how much they spend on cybersecurity (as a proportion of their overall spending on IT) and how successful their programs are.

What does a robust cybersecurity program look like? Our experience suggests that leading companies are working toward a state of digital resilience, in which they design their business processes and their IT systems to facilitate the protection of critical information and to implement strong cyberdefenses and effective plans for responding to cyberattacks. Seven practices are essential to achieving digital resilience:

1. *Include cybersecurity in management and governance processes.* Cyberrisk is a complex nonfinancial issue with the power to erode a company's bottom line and brand value. Because of this, companies need to integrate cybersecurity measures into day-to-day business processes and make cybersecurity a consideration in major decisions. For example, business units should make sure that only essential users can access customer information.

2. *Prioritize information assets and related risks.* At many companies, as much as 50 percent of information assets are not mission critical. Companies should take stock of their information assets, tally the cyberrisks they face and assess their urgency, and focus their cybersecurity efforts on mitigating risks to crucial assets. This can help them reduce their spending on cybersecurity by up to 20 percent.

3. *Strengthen cybersecurity protection for key assets.* Applying the same cybersecurity controls to all assets creates extra effort and expense. Vital assets should be protected more strongly than less important ones. Controls should go beyond typical options, such as encryption, to include authentication, access rights, data-loss prevention, digital-rights management, intrusion detection, and patching.

4. *Engage all employees.* Every employee has a part to play in protecting the enterprise through practices like sharing sensitive information through secure channels (rather than less-secure channels such as email). Phishing campaigns, cybersecurity drills, and other efforts will help make employees aware of cyberrisks and how to mitigate them.

5. *Build security features into IT systems.* Companies should build strong cybersecurity controls into the core of their IT systems. In-house software engineers should have the tools they need to develop applications that are less vulnerable to hackers. Companies should also configure IT systems in ways that reduce exposure to cyberrisks. For example, they can prevent employees from entering areas of computer networks that they do not need to use.

6. *Use "active defenses" to stay ahead of attackers.* Sooner or later, every company will be targeted by hackers. Companies can thwart hackers more effectively if they understand how hackers behave. Leading companies use big data analytics to identify signals that might indicate an impending attack, such as attempts to log in to networks from unusual locations. They also maintain up-to-date intelligence on cybercriminals' capabilities and intentions, and sometimes even their identities.

7. *Plan and test responses to cybersecurity incidents.* Knowing that cyberattacks will occur, companies should establish plans for responding to them. Once companies' incident-response plans are in place, they should regularly put them to the test in simulated cyberattacks, or "war games." Our research suggests that realistic simulations increase digital resilience.

Companies in Indonesia face the tough task of protecting their most important information, without making that information so difficult to access that it slows down their operations. Achieving digital resilience requires the involvement of multiple stakeholder groups. Oversight from the board and senior management is essential to ensure that cybersecurity programs are rigorous and effective. Dedicated cybersecurity teams must maintain a thorough, up-to-date understanding of the threats that companies face and engineer integrated defense systems to match. And business units and the IT organization need to embed security protocols in daily business processes. The stakes are too high for anything else. ■

This article is adapted from an article that appeared in the *Jakarta Post* on August 27, 2018, and is reprinted here by permission.

Vishal Agarwal is a partner in McKinsey's Singapore office, where **Aman Dhingra** is an associate partner and **Michael Gryseels** is a senior partner.

The authors wish to thank Yuza Setiawan and Shambavi Krishnamurthy for their contributions to this article.

Designed by Global Editorial Services.