Bridging the Cybersecurity Divide Between Large Enterprises and SMEs

In 1995, a report published by the National Telecommunications and Information Administration, an agency under the United States' Department of Commerce, examined the distribution of access to information and communication technology (ICT). It is from this report, "Falling Through the Net: A Survey of the 'Have Nots' in Rural and Urban America", that the phrase "digital divide" was coined and made popular by then Vice-President Al Gore.[1]

This term has since been used to describe the growing economic, educational, and social inequalities between populations with access to ICT and those without, both within and between nations. While it has been mostly used in this context, the same concept can also help us understand the differences between the haves and have-nots in the business environment. Enterprises with a higher digital maturity derive more revenue from their physical assets, are more profitable, and have higher market valuations.[2] Such success, however, is not achieved overnight—it requires enterprises to embark on a journey of digital transformation. According to the World Economic Forum's (WEF) Digital Transformation Initiative, such a transformation requires business leaders to undertake five action plans to be digitally ready.[3] These include re-skilling and transitioning the workforce, and creating new digital business models and digital offerings.

Significantly, one of the items is stepping up data security and privacy. Cybersecurity is a seen as a critical factor in the success and survivability of any digital enterprise. The WEF's Global Risks Report for 2017 ranks cyber risk—specifically "massive incident of data fraud/theft"—among the top five global risks.[4] It also forecasts digital enterprises to increase spending on cybersecurity from the current average of 1 percent of revenue to 3 percent over the next 10 years.[3]

---

[1] Richard Rapaport, "A Short History of the Digital Divide," *Edutopia by George Lucas Educational Foundation*, 2009, https://www.edutopia.org/digital-generation-divide-connectivity.
[2] Capgemi Consulting and MIT Center for Digital Business, "The Digital Advantage: How Digital Leaders Outperform Their Peers in Every Industry," 2012, https://www.capgemini.com/resources/the-digital-advantage-how-digital-leaders-outperform-their-peers-in-every-industry/.
[3] World Economic Forum and Accenture, "Digital Transformation Initiative Unlocking $100 Trillion for Business and Society from Digital Transformation," 2017, http://reports.weforum.org/digital-transformation/wp-content/blogs.dir/94/mp/files/pages/files/170328-dti-executive-summary-slideshare.pdf.
[4] World Economic Forum, "The Global Risks Report 2017 (12th Edition)," 2017, http://www3.weforum.org/docs/GRR17_Report_web.pdf.

This policy analysis has been written by Lim Wei Chieh and has been funded by the Lee Kuan Yew School of Public Policy (LKY School), National University of Singapore. The case does not reflect the views of the sponsoring organization nor is it intended to suggest correct or incorrect handling of the situation depicted. The case is not intended to serve as a primary source of data and is meant solely for class discussion.

This raises important questions for small and medium enterprises (SMEs), which have limited resources and budgets. Can they afford the high price of cybersecurity to ensure they can stay safe and survive in cyberspace? And, is there a cybersecurity divide between large enterprises that can afford state-of-the-art cyber defences across all aspects, from people and process to technology, and those that cannot? How would this divide, if it exists, impact industries and economic growth? What can be done to bridge this gulf?

In this paper, we examine these inequalities and their impact on SMEs, industries and nations, and the policies needed to ensure that SMEs are adequately secured in cyberspace against the backdrop of Singapore's push for SMEs to capture the growth opportunities in the digital economy.

SMEs at risk in an increasingly hostile cyber environment

As commerce moves increasingly online and governments come up with more incentives to go digital, a growing number of SMEs are starting to buy into the benefits of digitalising their enterprises. More than ever, SMEs are adopting ICT and exploring the use of advanced technologies, including big data analytics, artificial intelligence, and the Internet of Things. This has increased their exposure to cyber risks in today's hostile cyber environment.

A common misconception is that cyber criminals go only after large enterprises. While most SMEs might believe that they are not a target for cyberattacks, the reality is quite the opposite. In 2015, a U.S. House Committee on Small Business hearing called "Small Business, Big Threat: Protecting Small Businesses from Cyber Attacks" noted that 71 percent of cyberattacks happen to businesses with fewer than 100 employees.[5] A 2016 study on cybersecurity for SMEs by the Ponemon Institute in the U.S. also showed that 55 percent of companies suffered from cyberattacks while 50 percent had data breaches of customer and employee information over the previous 12 months.[6]

There are three key reasons for the higher cyber risks faced by SMEs.

1. SMEs have weaker cyber defences.

   SMEs that embark on digital initiatives without fully understanding and considering the associated cyber risks tend to allocate an insufficient budget to acquire and maintain adequate staff, management processes, and technology solutions to protect their digital operations and data.

[5] House Small Business Committee, "Small Business, Big Threat: Protecting Small Businesses from Cyber Attacks," April 22, 2015, https://smallbusiness.house.gov/news/documentsingle.aspx?DocumentID=398099.

[6] Ponemon Institute, "2016 State of Cybersecurity in Small & Medium-Sized Businesses (SMB)," *Ponemon Institute*, 2016, https://keepersecurity.com/assets/pdf/The_2016_State_of_SMB_Cybersecurity_Research_by_Keeper_and_Ponemon.pdf.

According to the Ponemon Institute's study, more than 60 percent of SMEs believe that their organisations are not effective in mitigating cyber risks, vulnerabilities, and attacks.[7]

While people are one of the key lines of cyber defence, employees in SMEs generally tend to have a lower understanding of cyber crimes and tactics. This is evident in their greater susceptibility to business email compromise (BEC) attacks, in which fraudsters spoof emails from C-level executives to financial staff requesting money transfers. According to Symantec, 38 percent of global victims of BEC attacks are SMEs, with the financial sector being the next largest at 14 percent.[8]

2. Size does not matter to cyber criminals.

While the cyber threat landscape is varied, ranging from ransomware and phishing to denial of services and targeted hacking, many attacks adopt a "spray and pray" approach and thus do not discriminate between organisations by size or industry. For example, the May 2017 WannaCry ransomware attack (that infected more than 200,000 machines across 150 countries) affected organisations both big and small in a wide range of sectors, including public services, telecommunications, transport, manufacturing, and education.

The most prevalent types of cyberattacks are also common across both large enterprises and SMEs. According to the Ponemon Institute's study, the top three types of attack experienced by SMEs are web-based attacks, phishing/social engineering, and general malware[9]—exactly the same top three cyberattacks suffered by all manner of organisations, according to the Verizon Business study of data breach investigations around the world.[10]

SMEs seem to be especially susceptible to malware and social attacks (phishing). According to Symantec,[11] for malware delivered over email, the rate for organisations with fewer than 500 employees is 0.920 percent on average, while that for larger organisations is 0.679 percent. And the phishing rate is 0.037 percent and 0.027 percent respectively. This means that smaller organisations are 35 percent more likely to receive email malware and 37 percent more phishing emails. (Table 1)

[7] Ibid.
[8] Symantec, "Billion-Dollar Scams: The Numbers behind BEC Fraud," July 12, 2016, https://www.symantec.com/connect/blogs/billion-dollar-scams-numbers-behind-bec-fraud.
[9] Ponemon Institute, "2016 State of Cybersecurity in Small & Medium-Sized Businesses (SMB)."
[10] Verizon Business, "2017 Data Breach Investigations Report (10th Edition)," 2017, doi:10.1017/CBO9781107415324.004.
[11] Symantec, "2017 Internet Security Threat Report," 2017, https://www.symantec.com/security-center/threat-report.

Table 1. Email Malware and Phishing Rate

Organisation Size	Email Malware Rate (%)	Phishing Rate (%)
1-250	0.787	0.035
251-500	1.053	0.039
501-1000	0.719	0.025
1001-1500	0.446	0.015
1501-2500	0.962	0.038
2500+	0.588	0.030

3. SMEs have valuable data and business relationships

   Although SMEs are smaller in scale, this does not mean that they do not have anything of value to cyber criminals. For example, the operations of even a small fintech company may involve the collection of sensitive personal information and processing of high-value financial transactions. Over a period of six months from July 2017, for example, data breaches in just six cryptocurrency platforms resulted in losses of more than US$50 million.[12]

   Cyber criminals also know that many SMEs have business relationships with larger organisations, and the weaker cyber defences in the smaller companies can provide a gateway into the bigger enterprises. For example, in the 2013 data breach of U.S. discount retailer Target Corp in which more than 41 million customer credit card records were stolen, it was discovered that hackers had broken in using access credentials stolen from a third-party vendor.[13]

Most SMEs do recognise the cyber risks they face. According to the Ponemon Institute study, more than 50 percent expressed concern that cyberattacks were becoming more targeted, sophisticated, and severe.[9] However, they said that meeting the cybersecurity challenge was tough as they had inadequate cybersecurity budgets (54 percent), staff (67 percent), and technologies (44 percent). A separate study by the U.S. Chamber of Commerce also highlighted the concerns of SMEs, with almost 60 percent worried of cyber threats.[14]

Business priorities and the cybersecurity budget challenge

In a study conducted by the Harvard Business School, board directors ranked keeping on top of risk and security issues as their biggest challenge, and said this was due to a lack of expertise and experience. Moreover, in a list of 23 board processes, only 24

[12] Waqas, "Hackers Steal $30 Million Worth of Cryptocurrency in Tether Hack," *HackRead*, November 21, 2017, https://www.hackread.com/hackers-steal-30-million-worth-cryptocurrency-tether-hack/.
[13] Kevin McCoy, "Target to Pay $18.5M for 2013 Data Breach That Affected 41 Million Consumers," *USA Today*, May 23, 2017, https://www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932/.
[14] U.S. Chamber of Commerce and MetLife, "Small Business Index Q3 2017," 2017, https://www.uschamber.com/sbindex/files/SBI_Q3_082217_REL.pdf.

percent rated their board process for managing cybersecurity responsibilities as "above average" or "excellent", which put this last in the list.[15]

In Singapore, cybersecurity—and technology investments, for that matter—is not seen as a business priority, especially among SMEs. According to the National Business Survey 2016/2017 conducted by the Singapore Business Federation (SBF), in which 86 percent respondents were SMEs, adoption of new technology and developing online business capabilities were ranked in the bottom quadrant of business focus for 2017.[16] Since cybersecurity spend is generally closely related to technology spend, it appears that SMEs tend not to allocate sufficient funds for cybersecurity.

It is important to recognise that there is a baseline budget required for minimum protection once an enterprise is connected to the Internet, for example, through email and web browsing. Perimeter defence, such as using network firewalls, to segregate and secure the enterprise environment from cyberspace is a basic requirement, and all PCs in a company should have enterprise-grade anti-malware protection installed. There should also be dedicated cybersecurity personnel—or at least IT staff responsible for securing the enterprise, including managing security vulnerabilities and keeping systems updated with the latest software. Often, SMEs do not have these basic minimum requirements in place and budget is a key obstacle; cybersecurity budgets also tend to be pegged to revenue or IT spend. A study conducted by the U.S. National Cyber Security Alliance and Symantec showed that 83 percent have no formal cybersecurity plan and 83 percent are not investing enough to protect customer data.[17]

Using the Singapore government's definition of a SME as having an annual revenue of less than S$100 million or employment size of less than 200 workers,[18] we can roughly estimate the cybersecurity budget for a SME with revenues of S$100 million.

Based on the CEB[19] CIO Leadership Council's IT budget benchmark report[20], the average IT spend of SMEs globally as a percent of revenue is 2.3 percent, but it can range from 0.8 percent to 7.9 percent in different industries and sectors. According to Gartner[21], organisations spend an average of 5.6 percent of their IT budget on IT security and risk management,[22] but the number can spread between 1 percent and 13

---

[15] J. Yo-Jud Cheng and Boris Groysberg, "Why Boards Aren't Dealing with Cyberthreats," *Harvard Business Review*, February 22, 2017, https://hbr.org/2017/02/why-boards-arent-dealing-with-cyberthreats.

[16] Singapore Business Federation, "National Business Survey 2016/2017 - Infographic," 2016.

[17] National Cyber Security Alliance and Symantec, "New Survey Shows U.S. Small Business Owners Not Concerned About Cybersecurity; Majority Have No Policies or Contingency Plans | Symantec," 2012, https://www.symantec.com/about/newsroom/press-releases/2012/symantec_1015_01.

[18] SPRING Singapore, "Factsheet on New SME Definition," accessed December 2, 2017, https://www.spring.gov.sg/NewsEvents/PR/Documents/Fact_Sheet_on_New_SME_Definition.pdf.

[19] CEB is a company providing advisory services and technology solutions, and serving more than 21,000 senior executives globally.

[20] CEB, "CEB CIO Leadership Council Key Findings from the IT Budget Benchmark," 2015, http://docs.media.bitpipe.com/io_10x/io_102267/item_465972/CEB%20IT%20Budget%20Benchmark%202015-16_MFV.pdf.

[21] Gartner is a technology research and advisory firm providing analysis and advisory services.

[22] "Gartner Says Many Organizations Falsely Equate IT Security Spending With Maturity," *Gartner*, December 9, 2016, http://www.gartner.com/newsroom/id/3539117.

percent. Putting the numbers together, we can observe that at the highest end, SMEs are spending approximately 1 percent of revenue on cybersecurity (Table 2), which is the average estimated by the WEF.[3] This means that most Singaporeans SMEs are spending below what WEF found to be the current industrial average.

Table 2. Estimated IT Spend for SMEs with S$100m revenue

	Low	Average	High
IT Spend as Percent of Revenue (%)	0.8	2.3	7.9
IT Security Spend as Percent of IT Spend (%)	1.0	5.6	13.0
IT Security Spend as Percent of Revenue (%)	0.008	0.129	1.027
Estimated IT Security Spend (S$)	8,000	128,800	1,027,000
Estimated IT Security Staff Cost (S$)	3,200	51,520	410,800

Studies indicate that a significant portion of SMEs' cybersecurity budget is spent on manpower costs. According to the CEB, approximately 40 percent of IT security budget is spent on staffing. To estimate the actual IT security headcount according to the human resources cost above, we can use Hudson's estimate that a cybersecurity professional with 8 to 12 years of experience will cost S$110,000 to S$160,000 annually, while one with more than 12 years of experience will cost S$160,000 to S$200,000.[23] This means SMEs employ between one and four professionals for IT security.

Table 2 gives us three possible categories of SMEs with the following (likely) profiles:[24]

1. **Low spend**: The SME has one IT staff member who spends a few hours a month seeing to cybersecurity issues, and the bare minimum in security technology (e.g. low-end network firewall and free antivirus software).

2. **Average spend**: The SME has one junior staff (likely with one to three years' experience), reporting to an IT manager, taking care of the company's cybersecurity needs. Spending on security technology may be adequate (e.g. enterprise network firewall, intrusion prevention, and commercial antivirus solution) but unlikely to meet the demands of a more complex technology environment and more sophisticated cyberattacks.

[23] Hudson Technology, "Salary Guide," 2017, http://hudson.sg/portals/sg/documents/SG Asia Talent Trends Technology SALARY GUIDE.pdf.

[24] We used a relatively simple approach in the above analysis to get an idea of the state of cybersecurity maturity of SMEs in Singapore. For a more accurate study, numerous factors must be considered, including industry sector, degree of digitalisation, stage of business growth etc. Available data in the public domain, however, is limited.

3. **High spend**: The SME has a dedicated security team with a manager and two to three staff members, and reasonable security technology protection from most cyber threats, except perhaps from persistent and determined cyber attackers.

Even at the highest level of cybersecurity spend, SMEs may still fall short of what is required in today's hostile cyber environment. In contrast, large enterprises enjoy economies of scale and can afford more sophisticated and costly cyber solutions, services, and professional staff.

Importance of addressing the cybersecurity divide

With 99 percent of enterprises in Singapore classified as SMEs, employing two-thirds of all workers and contributing half of Singapore's GDP,[25] the cybersecurity divide may have a significant impact on Singapore's drive towards a digital economy as well as overall cyber safety in Singapore. Three observations can be made:

1. Connectedness increases cyber risks

   The connected nature of the digital economy has increased the size of global trade, with 12 percent conducted over e-commerce.[26] With greater data flows between enterprises within their home country as well as between nations, cyber risks faced by one enterprise may be transferred across the supply chain network (e.g. through the spread of malware), as cyber criminals can hide within this data flow. Apart from using the communication network, they can also exploit the trust between business partners, suppliers, and buyers to cause harm across the business network (e.g. through compromising business email).

2. Digitalisation requires cybersecurity investment

   In line with its emphasis on the need to transform to a digital economy to drive greater growth and to stay ahead in the global economy, Singapore has come up with various programmes and initiatives to encourage and support SMEs on this transformation journey.[27] However, as shown earlier, increasing digitalisation without a corresponding increase in focus on cybersecurity can lead to greater exposure to cyber risk. This can affect the success of the SME programmes.

[25] Statistics Singapore, "Infographic on Singapore Economy," accessed December 5, 2017, http://www.singstat.gov.sg/statistics/visualising-data/infographics/economy.
[26] James Manyika et al., "Digital Globalization: The New Era of Global Flows," *McKinsey Global Institute*, February 2016, https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows.
[27] Committee on the Future Economy, "Strategy 4: Build strong digital capabilities." In Report of the Committee on the Future Economy, 2017, https://www.gov.sg/~/media/cfe/downloads/cfe report.pdf?la=en.

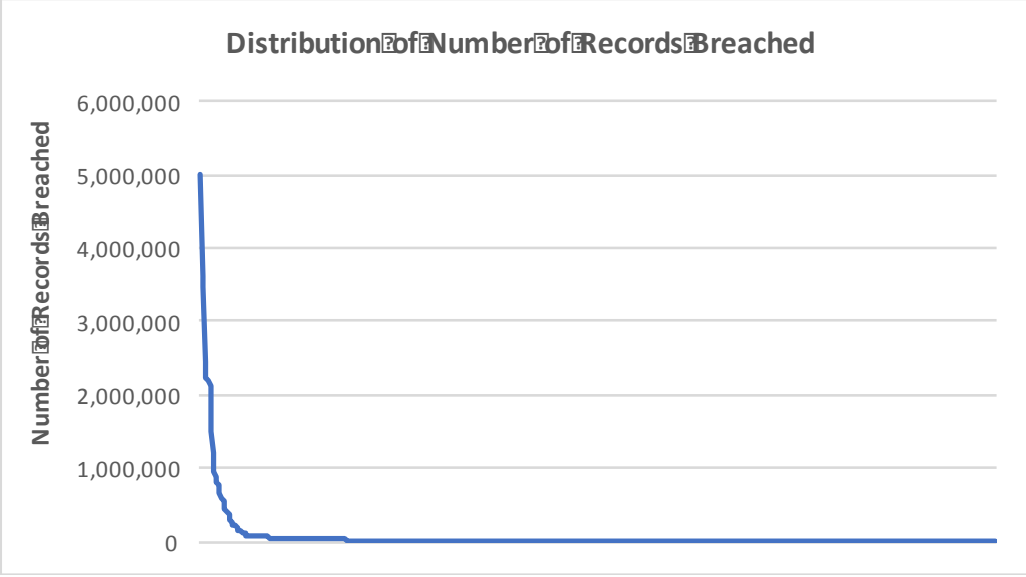
3. Cyber risks increase the burden on the economy

While massive data breaches make the headlines, there are numerous smaller data breaches that go unreported. But these breaches add up to significant cost to the country—both economically as well as reputationally as a trusted business environment. According to the U.S.-based Identity Theft Resource Center, 36.6 million data records were stolen in 2016.[28] The top 1 percent of breaches—those that tend to make the news—accounted for a loss of 18.9 million records, which is 51.7 percent of total losses. (Table 3) This means that the long tail of data breaches (the remaining 99%) can still result in significant damages, accounting for almost half of total data records lost. (Figure 1)

Table 3. Number of records breached by size

	Number of records breached	**Percent of records breached**
1% of data breaches	18,930,731	51.72%
99% of data breaches	17,671,208	48.28%
Total	36,601,939	100.00%

Figure 1. Breaches ranked by number of records breached



In the same way that improving public health benefits a nation's economy, improving the cyber health of SMEs can profoundly improve a nation's overall cyber risk profile and reduce the burden on its economy. This may become more critical as Singapore transforms to a digital economy.

Singapore government's support for SMEs

[28] Identity Theft Resource Center, "Data Breach Reports - 2016 End of Year Report," 2017, http://www.idtheftcenter.org/images/breach/2016/DataBreachReport_2016.pdf.

Unless there is government intervention, SMEs are likely to prioritise other business spending over cybersecurity, which is usually seen as a pure expense. Of the 34 grants and incentives offered to SMEs by Spring Singapore,[29] about 25 percent support business growth and expansion, 25 percent support productivity and innovation, 35 percent support manpower and training, and 15 percent support business transformation. From the author's analysis, only three grants/incentives can used for cybersecurity projects. These are:

1. Capability Development Grant (CDG): This can be used for to meet international ISO and Singapore's standards for information security, business continuity, and cloud security. SMEs can obtain up to 70 percent funding for qualifying project costs (until 31 March 2018 as of writing).

2. Critical Infocomm Technology Resource Programme Plus (CITREP+): This can be used to support information security and other ICT training. SMEs can obtain up to 70 percent funding for approved courses and certification fees, capped at S$2,500 per trainee.

3. Productivity and Innovation Credit Scheme (PIC): This can be used for training and expenditure on information security infrastructure equipment. SMEs can obtain 400 percent tax deductions for qualifying activities, or 40 percent cash rebates for expenditures up to a total of S$100,000 per year.

While training grants are useful and tax deductions can help defray the cost for equipment purchases, there appears, however, to be limited direct support for cybersecurity manpower costs. Besides, it is unlikely for SMEs to spend their limited cybersecurity budgets on standards certification, even with 70 percent funding support from the Singapore government.

In 2017, the Singapore government announced the SMEs Go Digital programme to help SMEs develop capabilities to exploit growth opportunities in the digital economy. The S$80 million programme, which supports the push for a stronger adoption of data analytics, artificial intelligence, and automation to accelerate the pace of economic transformation, provides up to 70 percent funding support, capped at S$300,000, for technology projects including cybersecurity and data protection. However, it should be noted that the current list of 69 pre-approved digital solutions (as of 6 November 2017) did not include any cybersecurity and data protection solutions.[30] SMEs will have to head to the SME Digital Tech Hub to get advice on these needs.

Even with the inclusion of support for cybersecurity and data protection solutions, it is unlikely that SMEs will use the fund for cybersecurity initiatives. Assuming a SME manages to obtain the maximum funding support of S$300,000, the total project cost

[29] SPRING Singapore, "Money Matters - SME Portal," accessed December 5, 2017, https://www.smeportal.sg/content/smeportal/en/moneymatters.html.
[30] Infocomm Media Development Authority, "SMEs Go Digital - List of Pre-Approved Digital Solutions," 2017, https://www.imda.gov.sg/-/media/imda/files/industry-development/small-and-medium-enterprises/smes-go-digital/list-of-preapproved-solutionssmes-go-digital-updated-as-of-6-nov-2017.pdf?la=en.

will still be less than S$430,000. And given business priorities, it is more likely that shortlisted SMEs will use the full amount for growth-related digital initiatives instead.

Government support needed for specific cybersecurity objectives

As outlined above, there remains a gap between the haves and the have-nots that needs to be addressed at a larger level. Just as the government needs to intervene to support SMEs through productivity and innovation incentives to fuel the growth engine of the Singapore economy, there must also be adequate support to secure this growth engine and manage the nation's cyber risk environment as more SMEs go digital.

To narrow the cybersecurity divide, the Singapore government may consider the following programmes to address the key challenges faced by SMEs in reducing their exposure to cyber risks:

1. Address top cyber threats to SMEs

   As noted earlier, SMEs face the triple threat of hacking, social attacks (e.g. phishing), and malware (e.g. ransomware. Increased support for the procurement of countermeasures, either through new programmes helmed by the Cyber Security Agency (CSA) or through additional specific funding support under current grants and incentives may help to address this.

   Larger enterprises can afford additional layers of cyber defence not commonly employed by SMEs, including threat intelligence, advanced anti-malware, breach prevention, and proactive monitoring solutions. By putting these solutions within the reach of SMEs, the government can upgrade the baseline cybersecurity capabilities.

2. Increase manpower support

   Manpower accounts for a significant portions of the cybersecurity budgets. Cybersecurity solutions need proper implementation by trained and experienced professionals.

   The current global demand for cybersecurity expertise has led to a shortage. According to the Global Information Security Workforce Study, There will be a shortage of 1.8 million cybersecurity professionals by 2022.[31] SMEs will be competing for scarce manpower resources with larger enterprises with deeper pockets.

   To level the playing field, Workforce Singapore (WSG) and the CSA could introduce a joint programme to provide salary support for qualified cybersecurity professionals.

[31] (ISC)^2, "Global Cybersecurity Workforce Shortage to Reach 1.8 Million as Threats Loom Larger and Stakes Rise Higher," June 7, 2017, https://www.isc2.org/News-and-Events/Press-Room/Posts/2017/06/07/2017-06-07-Workforce-Shortage.

3. Improve board-level awareness

   Awareness and training has always been a critical component of any successful cybersecurity programme. As highlighted earlier, board executives who do not fully appreciate the implications and possible consequences of cyber threats, and who have limited visibility of an organisation's cyber readiness may not make the right decisions in terms of priority and budget.

   The CSA could consider providing support for one-time threat and vulnerability assessments or cybersecurity maturity evaluation, which will help board executives understand the cyber risks and the state of their cyber defences. This top-down approach can help SMEs develop the right strategies for cybersecurity and prompt a re-examination of their cybersecurity budgets.

4. Mandate cybersecurity requirements for the SMEs Go Digital programme

   As more SMEs embark on digital initiatives supported by government grants and incentives, they will be exposed to more cyber threats. Without adequate cyber protections, these digital initiatives may result in costly data breaches, hampering broader digital strategies.

   Before SMEs get funding approval for projects with increased cyber exposures under the SMEs Go Digital programme, companies should be required to either demonstrate that they have adequate cyber defences or have included a cybersecurity component in proposed projects.

Over the past decade, cyberspace has grown much more hostile. With data breaches getting larger and more frequent, digital initiatives need to be supported by adequate cybersecurity protections.

As Singapore continues to push aggressively towards a smart city and with SMEs forming the backbone of the new digital economy, the widening cybersecurity divide between the 'haves' and 'have nots" must be closed to secure this digital future.