28

Digital Disruption: The SME Imperative

WILSON CHEW

Digital disruption is a phenomenon of the ages. Almost without anyone noticing it, it has irrevocably changed how companies and their boards view opportunities and challenges.

The catchphrase "disrupt or be disrupted" is a handy semaphore for what has become a battle of start-ups against incumbents. For incumbents, we tend to think of large companies. Video rental giant Blockbuster was caught unawares by Netflix and was bankrupted. Traditional taxi companies are eating Uber's dust. As if that is not startling enough, the average life span of an S&P 500 company – 65 years in the 1960s – is now around 15 years.

In this battle between David and Goliath, it is important to realise that small and medium-sized enterprises (SMEs) are not

spared. Examples also abound of SMEs that have been disrupted by competitors with new technology-enabled business models. The impact of Amazon's online book business on book-retailing giants like Borders and Barnes & Noble is well documented – as is the almost unnoticed demise of thousands of small and medium-sized brick-and-mortar bookstores around the world.

DIGITAL TRANSFORMATION: STRATEGIC IMPLICATIONS FOR SMES

The point is: digital disruption and the opportunity for digital transformation affects everyone, especially SMEs. The rules of competition have changed drastically, and so should the thinking of boards.

In this respect, the challenge for large companies lies not just in complacency, but also the sheer inertia involved in turning around a big ship.

SMEs, on the other hand, have fewer such issues. For starters, they are nimbler. They are less complacent since they must struggle to compete. They are also likely to spend proportionately more time studying their competitors and developing competitive advantage.

Therein lies the rub. In his book, *Competitive Strategy*, Michael Porter of Harvard Business School had, as early as 1980, warned of unexpected game-changers. In particular, he defined substitution as the availability of a product that the customer can purchase from another industry and thus reshape the competitive structure.

In other words, with technology, competition can literally come from anywhere in the world. The question "So, what else are our competitors doing?" is completely inadequate, if not dangerously shortsighted.

For example, many retailers in the South-east Asian region are (or will soon be) facing the threat of a new "Amazon". The Lazada Group was set up in Singapore in 2012 by Rocket Internet, a German incubator. The intention was to apply the Amazon business model to take advantage of the nascent online consumer market and Amazon's weak presence in the region. Today, Lazada's online presence in Indonesia, Malaysia, the Philippines, Singapore, Thailand and Vietnam sells inventory to customers from its own warehouses.

In this context, SME boards must embrace the reality that traditional operating models are going to be disrupted (if they have not been already). A renewed board agenda must involve a deeper discussion of strategy.

Some forward-looking SME boards practise pre-mortems. This is a scenario-planning process where the board and management work backwards from a hypothetical event of organisational failure to isolate the cause of that failure. There are two benefits: first, it identifies current assumptions that will be challenged going forward; and secondly, it produces a set of risks for the board to address.

Needless to say, the success of pre-mortems is contingent on how intellectually curious directors are, and on their ability to effectively engage with management. Those who bear strong domain knowledge with commercial skill sets will be able to contribute more.

DIGITAL DESTRUCTION: MASSIVE IMPLICATIONS FOR SMES

Cyberattacks are the other critical issue.

While the headlines fall on large-scale attacks the likes of Target, Sony and Apple, the fact is that SMEs are increasingly susceptible to cyberattacks. The 2015 Internet Security Report pointed out that 60 per cent of all cyberattacks are targeted at SMEs. They

are just as vulnerable as bigger companies to the theft of sensitive company information (customer details, trade secrets, and banking details), and the expensive and time-consuming consequences of lost sales, business disruption, fines, compensation, and recovery of lost assets.

Indeed, smaller companies are attractive to cyber criminals because they tend to have weaker online security. They also do more online business via cloud services that do not use strong encryption technology. In fact, some hackers find small companies a useful conduit or entry point into the network of a larger company to which the SME is a supplier.

Another increasingly common attack against small businesses involves ransomware. Here, the attacker installs malware on the victim's computer, and locks up data until a ransom is paid.

The point of this litany of alarming facts is that small businesses disregard the threat of cyberattacks at their peril. As fiduciaries, SME boards must include in their strategy agenda an effective cybersecurity plan that takes into account business continuity and crisis management.

To stay alive, SMEs need boards that keep ahead of the curve. They do this by being forward-looking, with their finger on the pulse of emerging technologies.

For starters, a company should consider inviting onto its board a director who can confidently deal with technology and cybersecurity issues. But beyond that, the board as a whole must be willing to strategise, follow through and directly address the challenges of digital disruption. ■