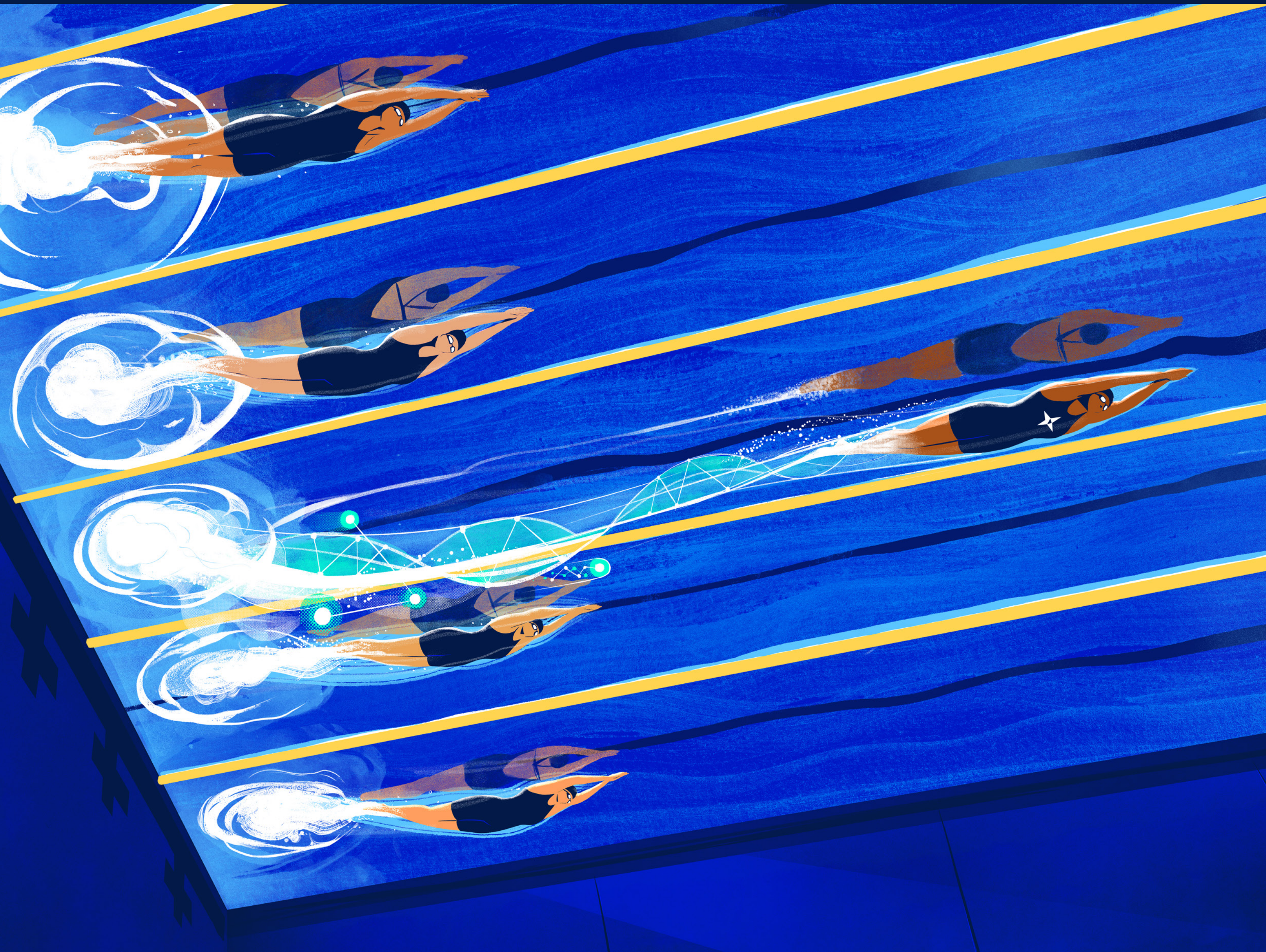
ISTARI Perspectives

Gaining Competitive Advantage from Cybersecurity

Manuel Hepfer

05 • 2021



Can cybersecurity be a source of competitive advantage? This seems like a brand new question, but it is not.

Forty years ago, at the dawn of the digital era, the business world asked a similar question about information technology. Although executives were pouring investment into IT, productivity gains proved disappointing. The 'IT productivity paradox' attracted business and academic attention.Some strategy consultants and researchers concluded that IT would quickly become a commodity; like electricity, it would be incapable of becoming a competitive differentiator.[i]

But the doubters were missing a key nuance. Yes, information technologies do not, in and of themselves, produce competitive advantage. However, the outcome is different when they are leveraged against a company's existing strengths. By the mid 1990s Wal-Mart, for example, began enhancing its massive distribution capabilities with IT, powering far ahead of its rivals. As others learned similar lessons, productivity took off. The lesson was that when deployed in combination with other company- specific capabilities and resources, IT does have the potential to contribute to a firm's competitive advantage.[ii]

The business world today is asking a similar question about cybersecurity. Many executives do not perceive cybersecurity as a strategic opportunity.[iii] Instead, they by and large see it as an operational necessity, a lose-lose situation. If their company is attacked, they will lose reputation and profit; if their company is not attacked, all that investment in resilience and prevention will be wasted. And although spending on cybersecurity increases every year, serious attacks keep succeeding. How then can organisations be resilient to cyber attack and use cybersecurity to improve their competitive advantage?

COMPANY RESOURCES AND COMPETITIVE ADVANTAGE

To answer that question, let us consider companies as a portfolio of resources.iv Resources are tangible or intangible assets of a firm, such as brand name, knowledge, production machinery, skills or technology. If a firm consistently outperforms its competitors, it is likely due to its superior portfolio of resources.

But competitors will try to imitate those high-performing resources, acquire them, or develop alternative resources that produce similar benefits. The strategic benefit of these resources diminishes. Only certain types of resources have the potential to produce long-lived superior competitive performance, a sustainable advantage that cannot easily be implemented by rivals. To achieve such sustainable competitive advantage, companies need to accumulate resource portfolios that create economic value, are relatively scarce, and can survive competitive imitation, acquisition, or substitution attempts.[iv] In other words, resources must be valuable, rare, inimitable, and non-substitutable to produce sustainable competitive advantage. Does cybersecurity meet these resource-based criteria for sustainable competitive advantage?

HOW TO GAIN COMPETITIVE ADVANTAGE FROM CYBERSECURITY

The answer to gaining competitive advantage from cybersecurity is similar to the solution of the IT productivity paradox. Companies aiming to gain sustainable competitive advantage from cybersecurity resources should make them valuable, rare, inimitable and non-substitutable. They achieve this by integrating their cybersecurity resources and strategies to leverage other company-specific complementary human, business, and technology resources – such as culture, organisational leadership, or learning capabilities. But how exactly does cybersecurity provide the basis for improving a company's competitive advantage? Traditional strategy theory, which focusses on strengths, weaknesses, threats, and opportunities, suggests that companies are able to improve their competitive performance only when their (valuable, rare, inimitable, non-substitutable) resources help them to neutralise threats or exploit opportunities. Cybersecurity strategy has the potential to do both.

At the bare minimum, companies should strive to neutralise

“Companies aiming to gain sustainable competitive advantage from cybersecurity resources should make them valuable, rare, inimitable and non-substitutable.”

serious cyber threats, and thus avoid competitive decline. Companies that experience a serious cyber attack can suffer from long-lasting impacts on their financial performance, customer trust, and reputation. Because serious cyber attacks often afflict only a single company within an industry, the attacked company suffers from competitive disadvantages. But worse is possible. In an interview I conducted, one CEO who has lived through a serious cyber attack stated, “Before the attack, it was completely impossible to think that anything could have the potential to put us out of business.” Mature cybersecurity protects companies from losing years of strategic effort and investment, and thus from suffering competitive disadvantages.

Most executives have recognised the need to neutralise cyber threats and to protect their business against cyber attack. But only a few have realised that mature cybersecurity strategy provides the basis for noticing, capturing, and exploiting strategic opportunities.

In my research at Oxford University, I spoke with executives who have started to view cybersecurity as a strategic asset. These leaders, having guided their company through a survival-threatening cyber attack, began using their cybersecurity accreditations to create new value propositions for customers. As more customers and partners in the supply-chain began to appreciate the value in conducting business with partners who were cybersecure, these companies began using that strength to win business and to improve their positioning in the market. One CIO told me, “We have won two significant bits of business and we won because we are one of the only companies that are accredited to security standards. That is starting to become a differentiator for us.”

Internally, companies can use cybersecurity as a lens to reveal new strengths and expose previously unnoticed weaknesses in other parts of the business, such as in manufacturing processes, leadership development or communications. My research found that companies with weak cybersecurity rarely did everything else right except for this one flaw. Cybersecurity strategy can expose these flaws in other organisational areas. One company leveraged cybersecurity strategy to reduce internal cost and to increase its speed of operation. Investments in cybersecurity transformed the company’s competitive position by standardising digital solutions across the company. A senior executive said, “Now, we can fundamentally move the company towards a fully digital business model.”

About the Author

Manuel Hepfer is a research analyst at ISTARI. Before joining ISTARI, he completed a DPhil (the Oxford equivalent of a PhD) in Cybersecurity and Strategic Management at the University of Oxford, where he was jointly affiliated with the Saïd Business School and the Oxford Centre for Cybersecurity. His research, which examines organisational resilience in the wake of cyber attack, won several awards.

i. Carr, N. G. (2003). IT doesn’t matter. Harvard Business Review.

ii. Powell, T. C., & Dent-Micallef, A. (1997). Information technology as competitive advantage: The role of human, business, and technology resources. Strategic management journal, 18(5), 375-405.

iii. Hepfer, M., & Powell, T. C. (2020). Make Cybersecurity a Strategic Asset. MIT Sloan Management Review.

iv. Wernerfelt, B. (1984). A resource-based view of the firm. Strategic management journal, 5(2), 171-180.

v. Barney, J. (1991). Firm resources and sustained competitive advantage.