



# A CEO and Investor's View on Cybersecurity and Resilience

---

CHIA Song Hwee  
Deputy CEO, Temasek International  
*Interview by Dr. Manuel Hepfer*

09 • 2021



## The Singapore investment company Temasek understands that as businesses accelerate their digital transformations, the danger of cyber attacks is greater than ever before.

By founding ISTARI, which brings together a portfolio of companies that offer cybersecurity products and services, Temasek aims to improve its cybersecurity posture and that of its investee companies.

CHIA Song Hwee, Deputy CEO of Temasek, recognises the growing cyber threats, and the less obvious benefits for companies that make cybersecurity a strategic asset. He believes that companies can turn their defensive investment in cybersecurity into business opportunities, but a mindset shift is required.

Manuel Hepfer, a cybersecurity researcher at ISTARI and Oxford University, had a chance to sit down with Song Hwee to learn how he has refined his thinking on cybersecurity, how he sees the topic as a CEO and investor, and what concerns him most.

*What follows is an edited version of their conversation.*

---

**MANUEL:** Over the past months and years, we have seen a number of high-profile cyber attacks. How have these altered your view on cybersecurity and resilience?

**SONG HWE:** Cyber risks have always been there, but never this intense and never this sophisticated. Many companies have accelerated their digitalisation initiatives and are reaching customers through digital platforms. That has created a fertile hunting ground for attackers.

However, many business leaders have not woken up to the seriousness of the issue. 15 years ago, you could just delegate cybersecurity to your IT guys and they would take care of it. But today, this can tarnish your good reputation and regulators may come after you, with huge fines to follow.

Yet, I have seen companies that have not yet made cybersecurity an agenda item for the board and the CEO. This may be because there is this illusion that it's "not going to happen to me". And the threat seems quite far away until you are attacked – or someone close to you is attacked. But that is naive thinking.

Of course, certain industries are more advanced than others. For example, I used to be a CEO in the semiconductor manufacturing industry. Even at that time, our equipment was pretty much fully automated. Therefore, any risk relating to our backbone in manufacturing was a key risk, just as safety was. So, whenever we talked about enterprise risk, cybersecurity was among the top issues.

Interestingly, what we didn't understand at the time was that what we were doing was actually creating a *competitive competency*. If you didn't have it, you didn't get to play.

I strongly believe that companies can turn investment in cybersecurity – what many only consider a cost – into an opportunity that generates returns. But it requires out of the box thinking. I'll give you a parallel example not in the cybersecurity space to illustrate the necessary change in mindset.

A few months ago, we had an opportunity to co-invest in a joint venture that converts passenger planes into cargo planes. One of the considerations in the debate was that because planes that burn fuel are not good for the environment, should we invest in that business?

I encouraged the team to think about turning that challenge into an opportunity. At first, they didn't understand what I meant. I said perhaps you could be the first freighter conversion company that helps customers to operate greener cargo planes. You cannot be totally green, but can you make the aircraft greener in the conversion process? When the joint venture launched, the emphasis on ESG and sustainability was the key differentiation. We had turned a challenge into an opportunity by helping the world reduce carbon emissions.



**MANUEL:** As an investor, how are you encouraging executives across your portfolio to transform their mindsets along these lines?

**SONG HWEE:** We are doing two things. The first is to lower the barrier for companies to adopt good cybersecurity practices by bringing in capabilities and tools at a cost that is easier to accept. For example, with IronNet, we created a collective defence mechanism, which we can bring to our portfolio companies and allow them to be a part of this cybersecurity “iron dome”. By aggregating the demand, we bring down costs for everybody.

The second is the research you do and training programmes from the ISTARI Academy that will raise awareness and bring people together. We need to create an environment where people feel comfortable sharing their experiences and challenges.

**MANUEL:** You mentioned operational, reputational, and regulatory risks. What do you worry about most?

**SONG HWEE:** At Temasek, we have been trying to identify the most vulnerable areas and to make appropriate risk assessments. Given the nature of our business, the risk we face is different compared to other operating companies. Certain vulnerabilities do not necessarily need to be addressed fully, because the business consequences are limited and you can accept them as being within your risk tolerance.

However, Temasek’s investment portfolio raises very different risks because we have hundreds of companies in our portfolio from around the world. In Singapore alone, we have companies that the government regards as critical information infrastructure.

Obviously, if something happened to these companies, we would have big problems. But, as shareholders, we clearly cannot get involved in the day-to-day activities of managing cybersecurity risk – that’s impossible. So together with ISTARI and the cybersecurity companies within the ISTARI portfolio, we want to create a solution to advance their cybersecurity risk management. We are still in the early stages of moving them in that direction, but we are making good progress.

**MANUEL:** As an investor, do good or bad cybersecurity practices make a difference in how you allocate investment?

**SONG HWEE:** I think that investors have a role in driving cybersecurity change, and this is quite similar to ESG initiatives. ESG is one of the many areas that we analyse in deciding whether or not we should invest in a company. And cybersecurity risk assessment is another. In several instances, we found that companies we wanted to invest in were vulnerable to cyber threats. Before we decided to invest, we highlighted to the management their cybersecurity issues and proposed how they could address them. In all cases, they have welcomed our suggestions and have acted on them.

And now, with the creation of ISTARI, we have many more capabilities, as an investor, to help companies become more resilient and protect their business value.

**MANUEL:** What is the role of the CEO in improving cybersecurity?

**SONG HWEE:** Even though this feels like a new challenge, it is not unique to cybersecurity. Decades ago, many companies in industries such as aviation, mining, or petroleum suffered from safety issues, but that’s no longer the case. Why? Because safety is very high up on the agenda of the CEO and the board. They have recognised that safety issues in operations can bring down your company. For example, decades ago, I used to be in an oil field. I wasn’t an engineer working in the field but I had to keep my safety passport up-to-date. I had to attend safety classes. I had been taught that when I walk down the stairs, I must hold the handrail. People got really, really good at safety. Not only operationally, but also in terms of their mindset and culture.

I believe that the same type of evolution will take place in the cybersecurity space. To drive that culture and mindset in cybersecurity, CEOs must empower their cybersecurity team and make them a respected part of the organisation.

Unfortunately, sometimes you need a disaster to change culture and mindsets. The question is, are people learning from what we see in the news, or are they waiting for disaster to befall them?

#### About the Authors

CHIA Song Hwee is the Deputy Chief Executive Officer of Temasek International. Prior to Temasek, Song Hwee was the Chief Operating Officer at GLOBALFOUNDRIES which has integrated with Chartered Semiconductor Manufacturing. Before the integration, Song Hwee served as Director of the Board, and President and CEO of Chartered Semiconductor from 2002 to 2009.

Dr. Manuel Hepfer is a cybersecurity researcher at ISTARI and Oxford University. Before joining ISTARI, he completed a DPhil (the Oxford equivalent of a PhD) in Cybersecurity and Strategic Management at the University of Oxford. His research, which examines organisational resilience in the wake of cyber attack, won several awards.