StrategicRISK

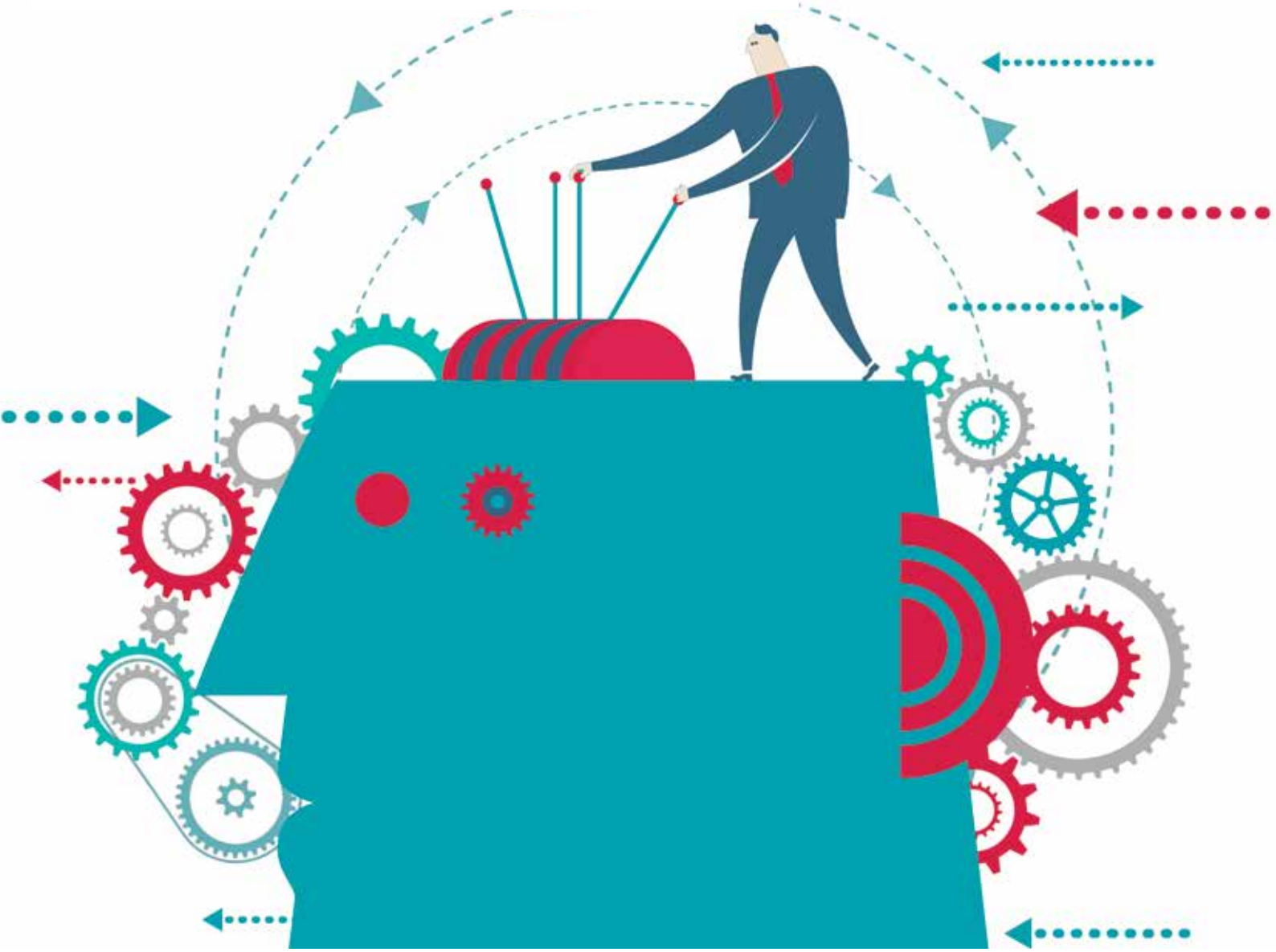
SPECIAL REPORT:

BUSINESS TRANSFORMATION

Our future is digital – there is no escaping it. Businesses that want to stay in the game must learn to adapt, with help from you, their risk expert. And this involves bolstering defences against the threats this new world will, inevitably, bring.

In association with

AIG



Drive the digital revolution

It is no longer optional. If businesses don't want to be left behind, they need a digital strategy. Risk managers may struggle to take the driver's seat but it is possible to steer the conversation.

Digital innovation can transform entire industries, practically overnight. Five years ago, not many of us would have turned to a ride-share company like Uber or Lyft for our journey home. Yet the Silicon Valley giants have transformed the transport sector in a flash, rendering minicabs nearly obsolete in some cities. Smart, nimble tech entrants have disrupted a host of other sectors in recent years, dominating retail, TV and food delivery. How many of us switch on Netflix instead of going to the cinema? Or opt for a Deliveroo rather than dining out?

As such, traditional business models have been redefined in the modern world. In an era of rapid digital transformation, companies risk being the next Blockbuster Video or Toys R Us, if they allow themselves to be left behind in the wake of digital innovation. Companies in every sector need to embrace digital developments, and risk managers should be part of assessing the landscape. But how involved are risk

managers in digital strategy? How are they responding to new ways of doing business? And what risks come with a digital transformation strategy?

A survey conducted by *StrategicRisk Asia-Pacific* and global insurer AIG reveals risk managers are yet to embrace digital innovation fully, with respondents saying they were yet to adopt key emerging technologies. Less than 80% of respondents have implemented cloud computing, while just 40% said their company used big data. Slightly more than 20% said their company used artificial intelligence.

Nearly 50% of risk managers said the risk function within their business had "little to no impact" on their company's digital transformation strategy. While 24% said the risk function was "not involved". A further 6% said they had an "insignificant" role. A total of 15% said they had a "minor" impact, and 52% said their involvement was "moderate".

What prevents risk managers from being involved in digital strategies? One risk manager said they had "nil representation or support with management". Another said: "Risk management is critical but is not always fully considered by IT teams." Another added: "Management does not treat risk management as important in their decision-making process."

The survey results reveal risk teams have more work to do to ensure digital transformation is viewed through a risk management lens. Without risk management input, companies could pursue dangerous strategies, or fall behind on innovation. Sector experts say risk teams must join the digital conversation.

50%
of risk managers said the risk function had "little to no impact" on digital strategy

NO PAST TO DWELL ON

Senior risk consultant Hans Laessoe, founder of AKTUS and former director of risk management at LEGO Group, believes "companies that do not leverage digitalisation run a significant risk of being obsolete – before they know it". He says every industry is at risk of being disrupted. "These technologies are spreading rapidly, but they are still in their infancy. Today online/mobile banking is common and not something we think much about – we just do it. Imagine an Uber or Airbnb of banking where blockchain technology makes the banking or money trading industry obsolete as everybody seamlessly deals with everybody without costly institutional 'middlemen'."

Patrick Smith is the global insurance and business resilience leader for online food delivery service Deliveroo. He warns companies in every sector to "digitally transform or die". He believes too many traditional companies are focused on old methods and short-term results, rather than looking to the future. Tech-driven start-ups do not have that burden, he notes.

"A key strategic decision for mature organisations is to balance the need to deliver short-term results funding outdated, or soon to be outdated, technologies, and to adopt a future-proof technology investment plan. The advantage start-up competitors have is that they are not faced with this choice."

Smith believes digital transformation will become even more pronounced in the next few years as customers expect an easy delivery of products and services. "Consumerism is king, and the end-user expectation is increasingly geared to technology-enabled execution; whether that be in retail, services or infrastructure and the connected home or workplace."

Digital transformation also brings new risks, changing the makeup of a company. Cyber risk is well-documented, but people risk should also be looked at differently, Smith says. "It is almost counterintuitive that the deeper we dive into the technology revolution, the more prominent people risk has become. The societal risk of skills redundancy is matched by the strategic risk of attracting and retaining the vital talents required to maintain, develop and create winning tech. The need to ensure that the talent is attracted to business building, rather than corporate disrupting activity, is vital."

Smith says companies need to focus on their strengths, despite the shift to new tech. "Organisations that completely migrate to a tech-enabled process may run the risk of ignoring the importance of judgement, sense-checking, gut-feel and experience. This change in skill base and expertise is highly likely to change the dynamic in any business, and arguably its culture and risk profile. The risk is potentially more crucial in the transitionary phase than it is to current or future states."

"COMPANIES THAT DO NOT LEVERAGE DIGITALISATION RUN A SIGNIFICANT RISK OF BEING OBSOLETE – BEFORE THEY KNOW IT."

Founder, AKTUS
Hans Laessoe

40%
use or plan to make use of big data in the next two years

IT'S OKAY TO TAKE THE PASSSENGER SEAT

How involved should risk managers be in the digital transformation process? Jeff Yao, an experienced risk practitioner based in Taipei, believes risk managers can play a central role. He says: "A good digital transformation strategy looks at both opportunities and threats. This is in the same spirit as transforming an organisation into a risk intelligent one. The role of a risk manager here is to remind leadership of that."

Yao believes digital transformation is not just for IT teams and boardroom decision-makers: "While the driver seat for a digital transformation may not be reserved for risk managers, the co-driver seat for a risk manager may not be a bad spot after all."

Our survey reveals risk managers' frustration at being frozen out of the conversation. How can risk managers become a bigger part of their company's digital strategy? Yao says risk managers have to be "plugged into the strategic planning processes and business decisions" made by the top team. "Through horizon scanning of potential risks, their mitigating measures can be shared, in real-time, with key decision makers."

Laessoe thinks it is not the risk manager's role to steer digital transformation but risk teams "should ensure that uncertainties are taken duly into account – both in terms of risks to mitigate, and opportunities to pursue". "They must analyse backwards to see what the consumer really wants and find new ways to provide that."

Meanwhile, Smith believes horizon scanning, and reporting insights to boardrooms will be valuable to companies. He says leading risk managers of the future "will become absolute experts in digital technology and its value to the business model and growth imperatives".

Smith adds: "Long gone are the days where digital technology and capability and its risks were the sole province of the IT department. The risk manager of tomorrow will become vital to strategic success by developing a leading understanding of digital opportunity, application and risk."

EXPERT VIEW: BE PROACTIVE IN PREPARING FOR THE INEVITABLE

Businesses are, albeit in some cases gradually, moving into the digital age. Risk managers must work to build a holistic team that can ensure strategies are successful and resilient to cyber crime, say AIG's Sheri Wilbanks and Liam Pomfret.

Sheri Wilbanks, Global Innovation Lead, AIG Client Risk Solutions

Liam Pomfret, Cyber Lead for Southeast Asia and New Zealand, AIG

Organisations of all shapes and sizes are on digital transformation journeys of varying degrees. Traditional business models are being transformed for the digital age and technology start-ups are bringing new and fierce competition to the marketplace. Digital strategies are being developed in response and the question is, what role should risk managers play here?

Our survey developed with *StrategicRISK* suggests that a healthy proportion of businesses are currently or plan on using new and advanced technologies – cloud computing, big data, the internet of things (IoT), automation and AI; but only 50% say that risk management has a moderate impact on ensuring that their company's digital transformation strategy is successful.

Our view is that risk managers play a vital role to this strategy. They have an overarching and holistic view of the organisation's potential risks and vulnerabilities, including regulatory implications for a specific digital or technological choice, and will have insight on emerging trends. These form an important part in ensuring the resilience of a company's digital transformation strategy.

And as more businesses become digitally advanced, their vulnerability to cyber-related attacks will likely increase. Take data breaches as an example. Most departments within an organisation will generate or house some form of data: whether it is finance, who may collect and have access to sensitive customer information; or HR who may collect personal information on members of staff.

As the conduits for effective risk management across the business, risk managers will be able to assist technology colleagues in mapping their critical data assets and identifying vital information: who has access to what data; what level of authority and permissions have been granted to who; and do business partners have access.

Cyber risks have also evolved, becoming more complex and interconnected as technologies such as the IoT, AI and automation gain momentum within businesses. Attacks can manifest in several ways, widening the scope of damage causing, for example, damage to reputation, business interruption if critical systems are shut down, and physical damage.

Cyber criminals are highly motivated, well-resourced and appear to be one step ahead of the curve. They have the capabilities to take control of entire systems, causing fires, physical property damage and injury. They can infiltrate systems and change critical codes or recipes, or release goods to the wrong people. And they can steal data and publicly share sensitive customer details, as was the case with SingHealth.

21st century cyber-attacks are fast-evolving and extend far beyond financial damage. And unlike some traditional risks, cyber threats and the associated controls need to be assessed regularly to keep up with the relentless onslaught of new threats. Indeed, managing the risks calls for a holistic and joined-up team, made up of internal stakeholders and external experts, including IT forensic personnel, lawyers and crisis communication.

Insurers play a critical role here and are evolving their solutions to ensure they are fit for the complexity of cyber risks. Many of their solutions now provide access to critical teams made up of the external experts mentioned above.

AIG has gone a step further with its policies and wordings, which have been written to include protection against physical damage. We have provided cyber-related solutions for the past decade and pride ourselves on our end-to-end support. This includes helping risk managers measure and model cyber risk in economic terms via proprietary tools; and assist in planning for what seems to be the inevitable.

At AIG, we see ourselves as a key member of a risk manager's holistic team as they progress through their digital transformation journey.

Don your cyber armour

A cyber attack can be crushing. Yet three-quarters of risk managers surveyed say their business does not having a cyber response plan ready to go in the event of a disaster. Don't be fooled – it can happen to you.

Cyber risk poses an immediate threat to companies all over the world. Highly visible and malicious attacks occur with alarming regularity, making cyber risk one of the most challenging issues for risk managers today. It can take months, or even years, for companies to recover from a single cyber attack, with huge financial damage and operational disruption.

The Asia-Pacific region has seen several high-profile cyber attacks in 2018, including the significant breach of Singapore's health system in July, which affected 1.5 million people.

A devastating attack also hit Hong Kong airline Cathay Pacific earlier this year. During the attack, details of 9.4 million Cathay Pacific customers were stolen, including passport numbers, dates of birth, and Hong Kong ID data.

Attacks cause significant financial and reputational damage, and the fall-out from an event can spiral quickly out of control. Yet, despite an ever-growing number of attacks, a recent study conducted by *StrategicRISK* and AIG reveals many companies do not have preventative measures or a response plan in place. In the face of increasingly sophisticated cyber risk, are companies prepared for the inevitable, or burying their heads in the sand?

HEAD IN THE SAND

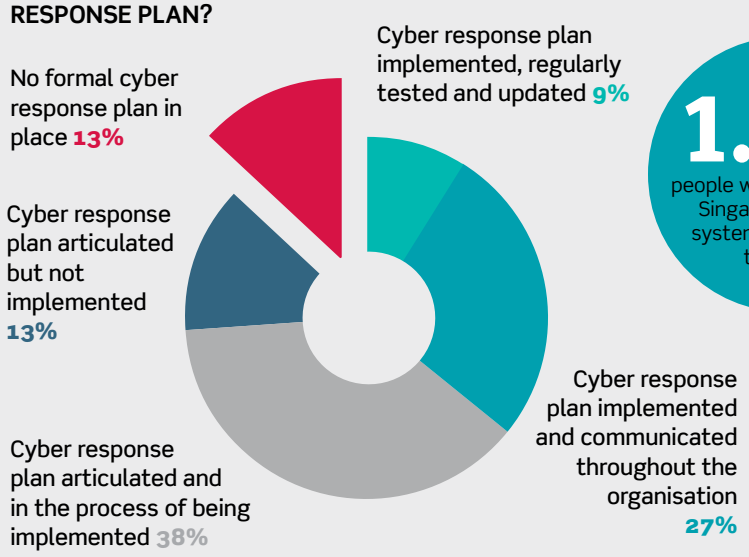
According to our survey, 13% of companies have no cyber response plan. A further 13% said their plan was "articulated but not yet implemented". While 38% said their cyber response plan was "in the process of being implemented". Just 27% said they had a well-developed and rehearsed response plan.

Risk managers are also reluctant to use cyber insurance. Two out of five risk managers said they had no plans to take out a policy, while just 22% have coverage.

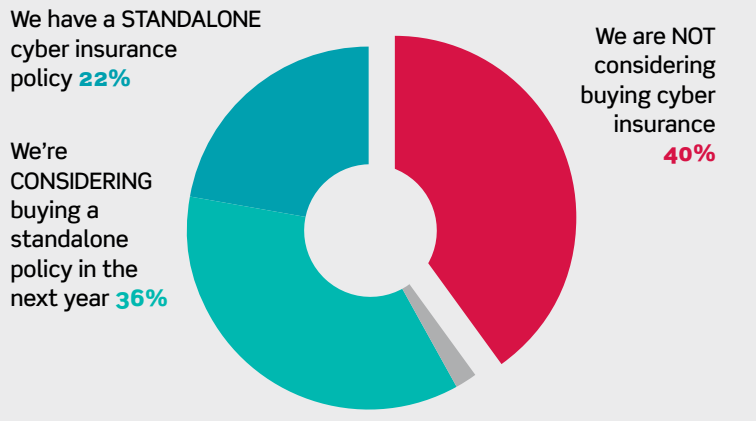
SURVEY: HOW SERIOUSLY IS CYBER RISK VIEWED IN YOUR BUSINESS?

Results from *StrategicRISK* and AIG's cyber risk survey reveal a lacklustre attitude for implementing a risk response plan, and unwillingness by many businesses to commit to a specific cyber risk insurance.

HOW WOULD YOU DESCRIBE YOUR CYBER RISK RESPONSE PLAN?



WHAT ROLE DOES CYBER INSURANCE PLAY IN YOUR RISK MITIGATION STRATEGY?



We HAD a standalone policy but have not renewed/do not plan to renew 2%

1.5m people were affected by Singapore's health system data breach this year

Paul Looker, former risk manager at job search website Seek, and now chief executive of risk consultancy Cybassurance Pty, says there is a "general sense from organisations, both large and small, that they will not be a target". He says this "de-prioritises cyber risk, and therefore the need for a cyber incident response plan".

But Looker warns cyber attacks go far beyond financial damage and IT disruption. "Apart from direct financial loss, cyber attacks can drain significant time and energy from an organisation, which has an often significant opportunity cost." He adds reputational damage can have a long-term impact, while poorly handled cases can have "flow-on effects".

KEEP IT BASIC, BUT KNOW IT

How do companies ensure they have the right controls in place? Looker says businesses need to conduct cyber risk assessment and remediation work and have their assessment audited by an independent third party, to "truly understand residual risk".

Well-prepared companies are likely to minimise damage when an attack hits. Craig Searle, the co-founder of cybersecurity consultancy Hivint, says businesses should have "basic" and "non-negotiable" strategies in place.

He adds: "Fundamental controls don't require large investments, and when implemented correctly, go a long way to mitigating exposure. Things like application whitelisting, multi-factor authentication, and proper patching procedures might not be the sexiest security strategies, but they work."

Searle says risk managers should tailor their cyber control and response plans, and become part of the conversation in their business. "This is where risk managers can take the lead and identify the specific organisational issues that require additional investment."

Susie Jones, co-founder of Cynch Security, and former risk manager at Australia Post, says the Office of the Australian Information Commissioner is a useful source of cyber response tips. While planning and procedure are crucial, Jones says staff need to be well-versed in their company's response plan.

"The most important point to remember when considering cyber risks and response plans is that people are at the centre of everything. This means that you should test the plans thoroughly and often. Every time a person noted in your plan leaves or changes role, it should be tested."

Jones says testing should "become second nature to more than just your response team". She adds: "This means dedicating the time to teaching everyone involved how to act, without needing to refer to a document."

Jones says our survey results highlight "a disconnect between general risk managers and those responsible for cybersecurity within these corporations". She adds: "One potential reason for this is the common belief that by moving technology off premises and to a cloud solution, the risk is transferred outside of your sphere also. This is simply not the case."

"Risk managers need to help their business to realise that the risk doesn't transfer with cloud adoption, but at best transforms into a new set of risks they still need to manage. There have been a number of well-publicised data breaches this year that have highlighted this dangerous belief in the ability to outsource cyber risks to third parties."

"IT IS THE COMMON BELIEF THAT BY MOVING TECHNOLOGY OFF PREMISES AND TO A CLOUD, THE RISK IS TRANSFERRED OUTSIDE OF YOUR SPHERE. THIS IS SIMPLY NOT THE CASE."

Co-founder,
Cynch Security
Susie Jones

PROTECT YOURSELF

Insurance can also play a role in helping risk managers combat cyber risk. Jones says insurance policies do "begin to address" cyber risk. But cyber insurance is just one part of the solution, "amongst a raft of controls that a business needs to have in place".

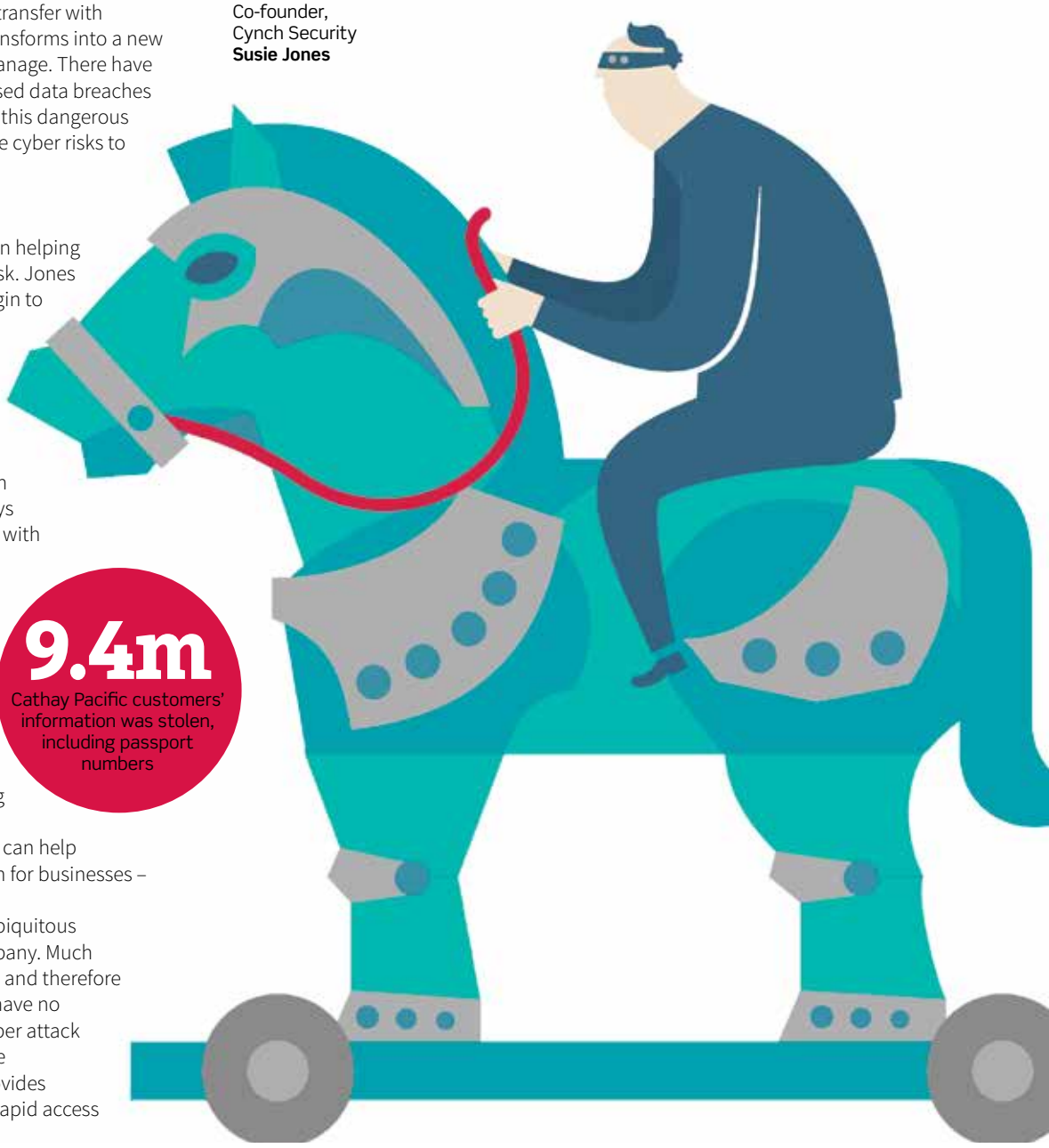
Peter Jackson, senior director, Asia region, at Lockton Wattana Insurance Brokers, says insurance can help companies with cyber controls as well as their response plan.

"Many insurers offer breach support services and breach prevention advice. More could be done to make clients aware, not only of the overall risk, but of emerging cyber risks, which are changing all the time."

9.4m
Cathay Pacific customers' information was stolen, including passport numbers

Jackson believes insurance can help add another layer of protection for businesses – before it is too late.

"Cyber is one of the most ubiquitous risks, facing almost every company. Much of what happens is out of sight and therefore out of mind. Most companies have no experience of what a major cyber attack is like until they experience one first-hand. Cyber insurance provides both financial protection and rapid access to expertise."




Insuring the impossible.
In an ever-changing world, AIG empowers clients to embrace every new opportunity. Discover personalized insurance solutions powered by the latest technology, innovative partnerships, and industry-leading experience.
AIG
Bring on tomorrow®
Insurance, products and services are written or provided by subsidiaries or affiliates of American International Group, Inc. Insurance and services may not be available in all jurisdictions, and coverage is subject to actual policy language. For additional information, please visit our website at www.AIG.com.