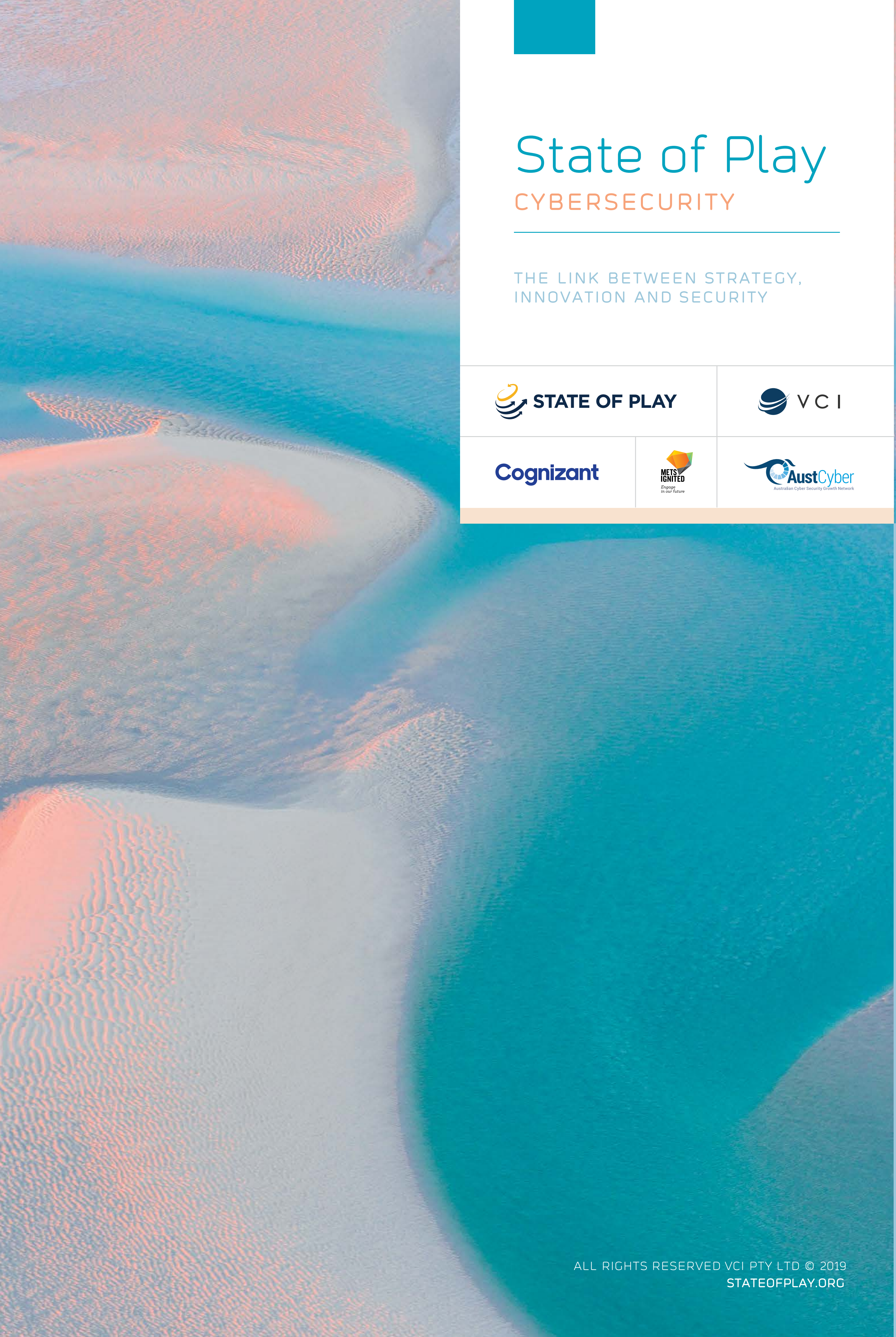


State of Play

CYBERSECURITY

THE LINK BETWEEN STRATEGY, INNOVATION AND SECURITY

STATE OF PLAY

VCI

Cognizant

METS IGNITED
Engage in our future

AustCyber
Australian Cyber Security Growth Network

STATEOFPLAY.ORG

About State of Play

The State of Play platform was initiated by VCI in partnership with The University of Western Australia in 2011 and is now the largest mining research platform on strategy and innovation in the world. Our ambition was to create a platform to support industry discussion of innovation and performance at a strategic level, develop macro-level insights into the industry ecosystem, and more clearly articulate effective strategy execution and business design for the industry.

Since its inception, State of Play has surveyed several thousand mining and service company senior executives across six continents and over a hundred countries, developing over a million individual data points over time that paint a diverse and fascinating picture of the industry and its evolution.

State of Play chose to research cybersecurity in mining late in 2018 as we were conducting interviews for our main biennial report on strategy and innovation in mining, now the largest and oldest in the industry. Many of the executives we spoke with were raising cybersecurity as a strategic consideration at a far higher rate than in years gone. Further, several asked if we were going to look at it specifically as one of the largest strategic risks facing the industry.

So, it was as strategists that we have approached this research, and we've been hugely taken by the sheer amount of investment and innovation on both sides of the cybersecurity fence. In all, it has been a fascinating year of research, interviews and analysis.

State of Play: Cybersecurity represents a specific drill-down report independent from the major strategy and innovation research. In this it continues the path set by the State of Play: India and State of Play: South Africa reports and expected to be built on with the upcoming State of Play: Venture capital report.

All State of Play reports and data packs are available at: www.stateofplay.org.

KEY RESEARCH STATISTICS:

EXECUTIVE INTERVIEWS: 11

CONTINENTS: 6

RESPONSES: 100

Including 5 Board members, 11 CEOs, 1 CSO, 3 COOs, 14 CTOs, 8 CISOs and Business Unit Heads with approximately 50% from, 40% services companies and 10% from government and academia.

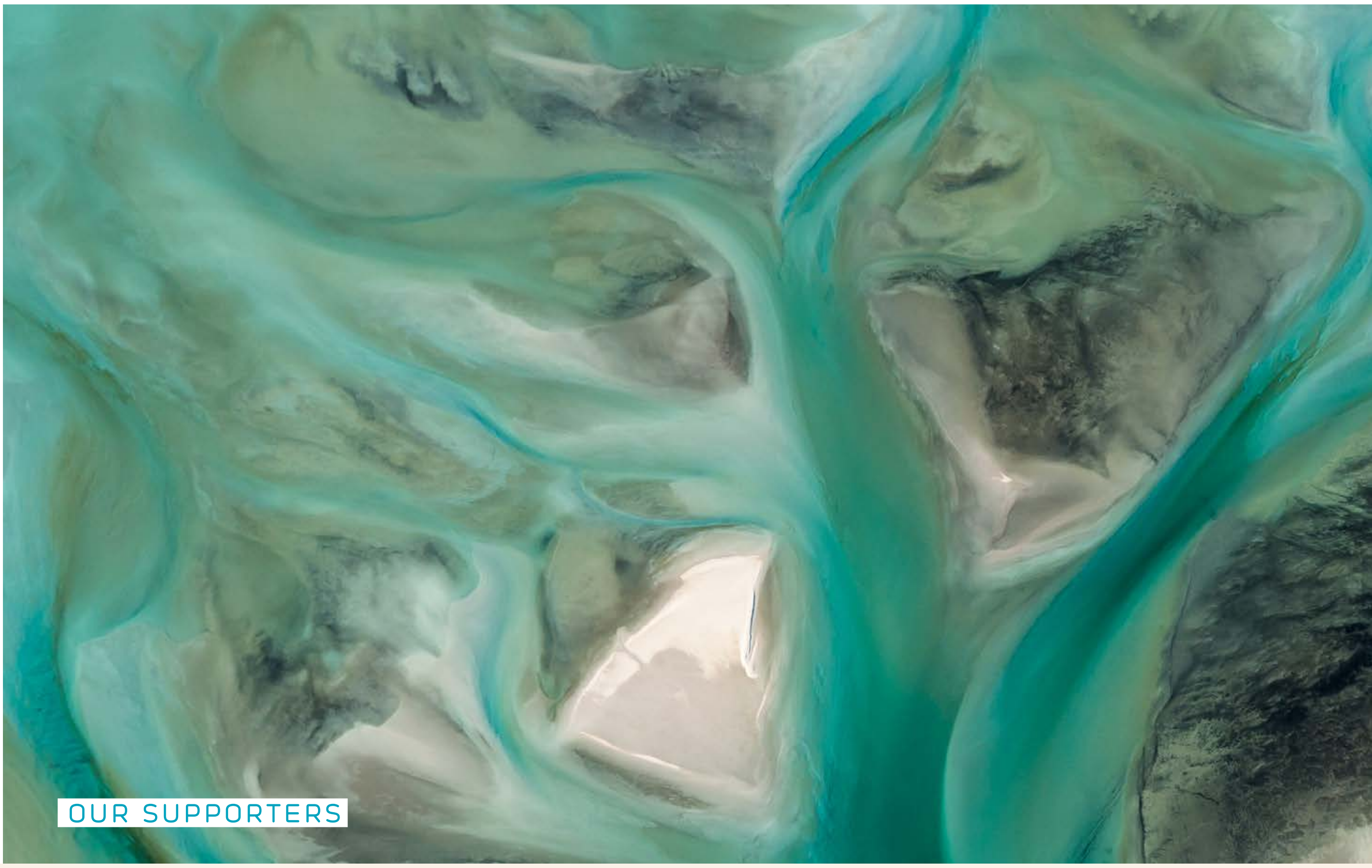
VCI and its logo are trademarks of VCI. This document is produced by VCI as general guidance. It is not intended to provide specific advice on your circumstances. If you require advice or further details on any matters referred to, please contact a VCI representative.

Authors

Graeme Stanway
Paul Mahoney
Kevin Ong

Contributors

Helena Trang
Stephanie Munro
Madi Ratcliffe
Xavier Evans
Joelle Chan



OUR SUPPORTERS

VCI

VCI is a global management consulting company that focuses on the resources industry. Our core focus areas are strategy, innovation and organisation. We work with senior leaders to overcome their most difficult and pressing challenges with a collaborative and open approach. VCI has built its reputation based on a deep curiosity and applying creative methods to difficult problems.

Graeme Stanway, CEO and Co-Founder
Paul Mahoney, Principal

www.govci.com

Cognizant

Cognizant is one of the world's leading professional service companies, transforming clients' business, operating and technology models for the digital era. Their unique industry-based, consultative approach helps many of the best-known organisations in every industry and geography envision, build and run more innovative and efficient business.

Kirby Johnson, Global Client Partner
Warwick Hill, Global Client Executive
David Stevenson, Senior Director

www.cognizant.com

METS Ignited

METS Ignited works with Australian suppliers to the mining industry, global miners, research organisations and capital providers to improve the global competitiveness and productivity of the Australian METS sector. Its five areas of strategic focus to help strengthen the global competitiveness of the Australian METS sector are: a shared vision; strengthening collaboration in the mining innovation system, addressing gaps in the METS-Mining ecosystem, raising the profile of the METS sector, and promoting world-class clusters.

Adrian Beer, CEO
Ian Dover, General Manager
Peter Clarke, General Manager

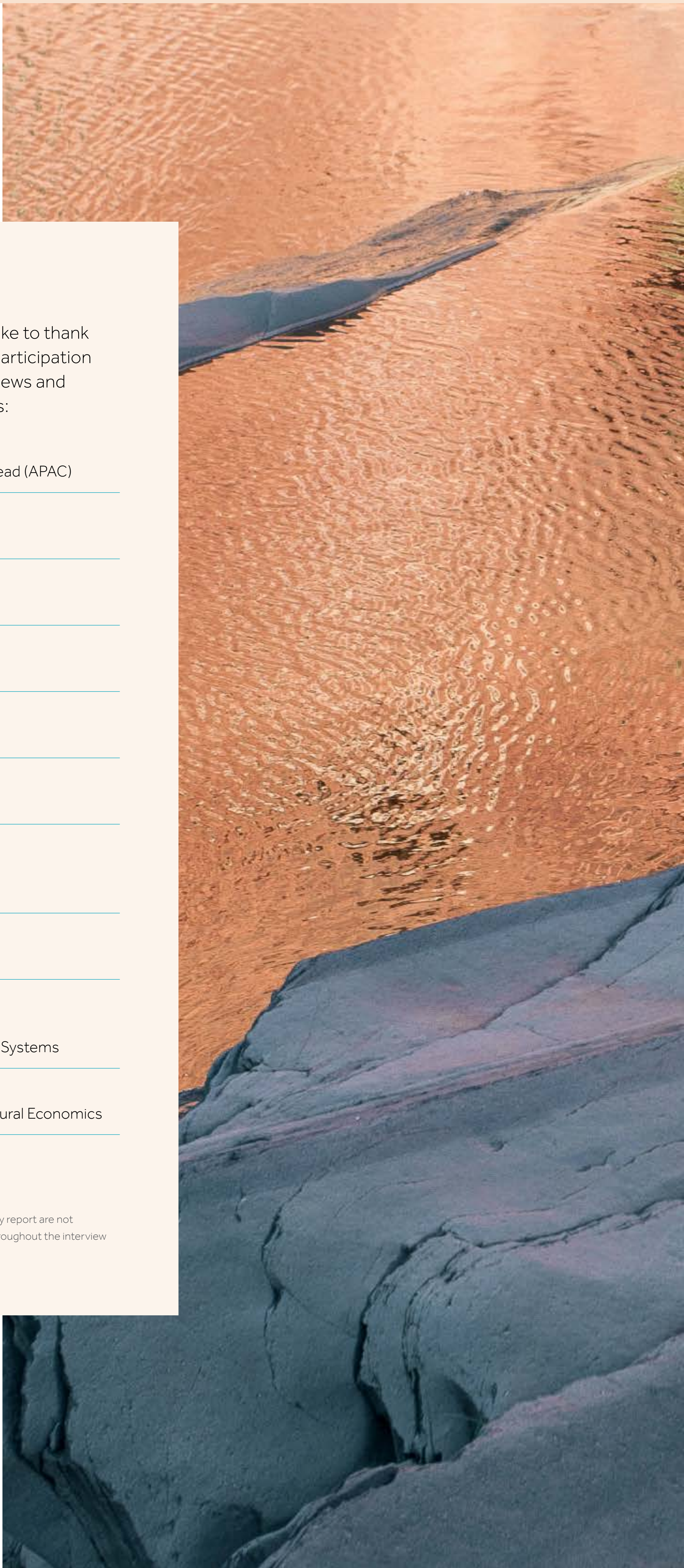
www.metsignited.org

AustCyber

AustCyber exists to grow an Australian cyber security ecosystem, export Australia's cyber security to the world, and make Australia the leading centre for cyber education. Their program of activities are underpinned by evidence gained through extensive research and consultation. Their flagship Sector Competitiveness Plan and Industry Roadmap outline the opportunity for Australia's cyber security sector to support growth across the whole economy.

Michelle Price, CEO
Prerana Mehta, Chief of Ecosystem Development
Mike Bareja, Program Director Innovation and Capability Growth

www.austcyber.com



PARTICIPANTS

The State of Play team would like to thank the following people for their participation in this research through interviews and interpretation of survey results:

AngloAmerican
Daryl Chew, Information Security Head (APAC)

BankVault
Graeme Speak, Founder & CEO

BHP
Thomas Leen, CISO

Black & Veatch
John Voeller, Former CTO

Diamond Cyber
Sven Ross, CEO

Gold Fields
Strini Mudaly, CIO

MM-ISAC
Rob Labbé, Chairman
Cherie Burgett, Director

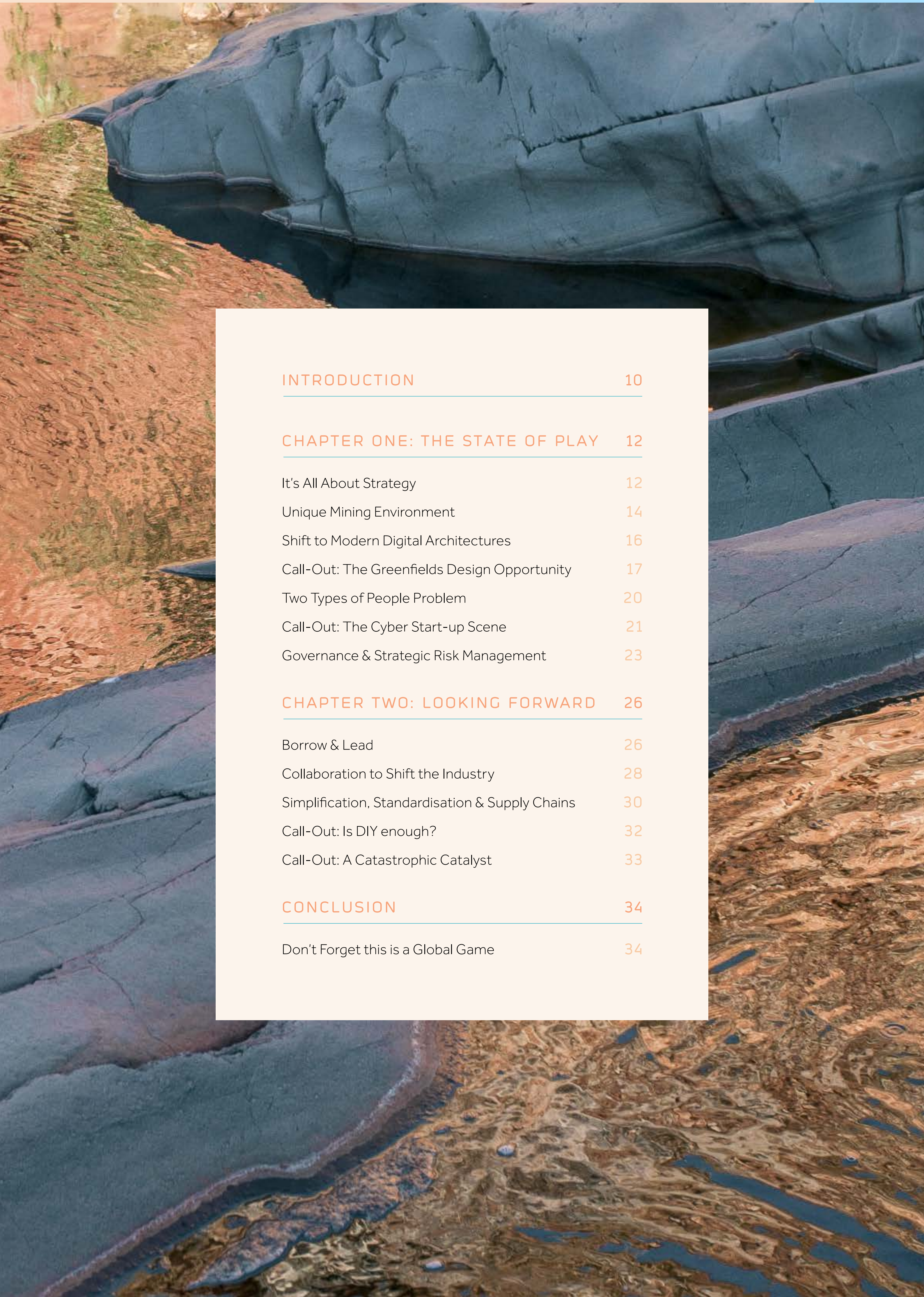
SINET
Robert Rodriguez, CEO

South32
Clayton Brazil, CISO
Johan Coetzee, Director Operating Systems

University of Texas
Kay-Yut Chen, Professor of Behavioural Economics

Woodside Petroleum
Andrew Melouney, CISO

Quotes throughout the State of Play: Cybersecurity report are not individually attributed. All quotes were collected throughout the interview series with the executives listed above.



RECENT GLOBAL CYBERSECURITY BREACHES

November 2019

UK Labour Party hit by "sophisticated and large-scale cyber-attack on its digital platforms" ahead of elections. The attack aimed to flood Labour party online platforms with various sources to slow down access or cause their websites to crash.

October 2019

India's newest nuclear power plant was the victim of a cyber-attack. The hack used malware designed for data extraction and cyber security experts say critical information was compromised.

September 2019

Huawei accused the U.S. government of hacking into its intranet and internal information systems to disrupt its business operations.

August 2019

Chinese state-sponsored hackers were revealed to have targeted multiple U.S. cancer institutes to take information relating to cutting edge cancer research.

August 2019

The Czech Republic announced that the country's Foreign Ministry had been the victim of a cyber–attack by an unspecified foreign state.

August 2019

A seven-year campaign by an unidentified Spanish-language espionage group was revealed to have resulted in the theft of sensitive mapping files from senior officials in the Venezuelan Army.

July 2019

Capital One reveals that a hacker accessed data on 100 million credit card applications, including Social Security and bank account numbers.

July 2019

Encrypted email service provider ProtonMail was hacked by a state-sponsored group looking to gain access to accounts held by reporters and former intelligence officials conducting investigations of Russian intelligence activities.

July 2019

Several major German industrial firms including BASF, Siemens, and Henkel announced that they had been the victim of a state-sponsored hacking campaign reported to be linked to the Chinese government.

July 2019

Microsoft revealed that it had detected almost 800 cyberattacks over the past year targeting think tanks, NGOs, and other political organizations around the world, with the majority of attacks originating in Iran, North Korean, and Russia.

July 2019

The U.S. announced it had launched offensive cyber operations against Iranian computer systems used to control missile and rocket launches.

June 2019

Almost 100,000 Australians' private details exposed in attack on Westpac's PayID.

June 2019

Chinese intelligence services hacked into the Australian National University to collect data they could use to groom students as informants before they were hired into the civil service.

May 2019

Software update crashes police ankle monitors in the Netherlands – Borked update prevents ankle monitors from sending data back to police control rooms. Some suspects needed to be collected and sent back to jail as a result.

May 2019

Australians Medicare details illegally sold on darknet – two years after breach exposed.

May 2019

A surveillance contractor for US Customs and Border Protection suffered a breach, and hackers stole photos of travellers and license plates related to about 100,000 people.

May 2019

WhatsApp urges users to upgrade app after discovering spyware vulnerability.

April 2019

Puma Australia shoppers hit with credit card hack.

April 2019

Microsoft admits Outlook.com hackers were able to access emails.

April 2019

Pharmaceutical company Bayer announced it had prevented an attack by Chinese hackers targeting sensitive intellectual property.

March 2019

The American Medical Collection Agency, a massive health-care-related debt collector discovered that an intrusion on its systems lasted from August 2018 through March 2019.

March 2018

Norwegian aluminium maker Norsk Hydro may have lost more than $40 million in the week that followed a cyber-attack.

February 2019

Attempted cyber-attack on Australian parliament.

February 2019

LandMark White Data Breach-Home loan details of 100,000 customers hacked in major data breach.

January 2019

Private equity firm, Rhodes & Beckett, alleges website 'held to ransom'.

January 2019

Hackers release the personal details, private communications, and financial information of hundreds of German politicians, with targets representing every political party except the far-right AfD.

January 2019

Nyrstar has been subject to a cyber-attack, which has led to certain IT systems, including email, being shut down across its headquarters in Zurich, Switzerland, and, globally, at the metals processing and mining operations.

January 2019

Italian oil company Saipem was targeted by hackers utilizing a modified version of the Shamoon virus, taking down hundreds of the company's servers and personal computers in the UAE, Saudi Arabia, Scotland, and India.

INTRODUCTION

"Cybersecurity touches everything, it is like breathing."

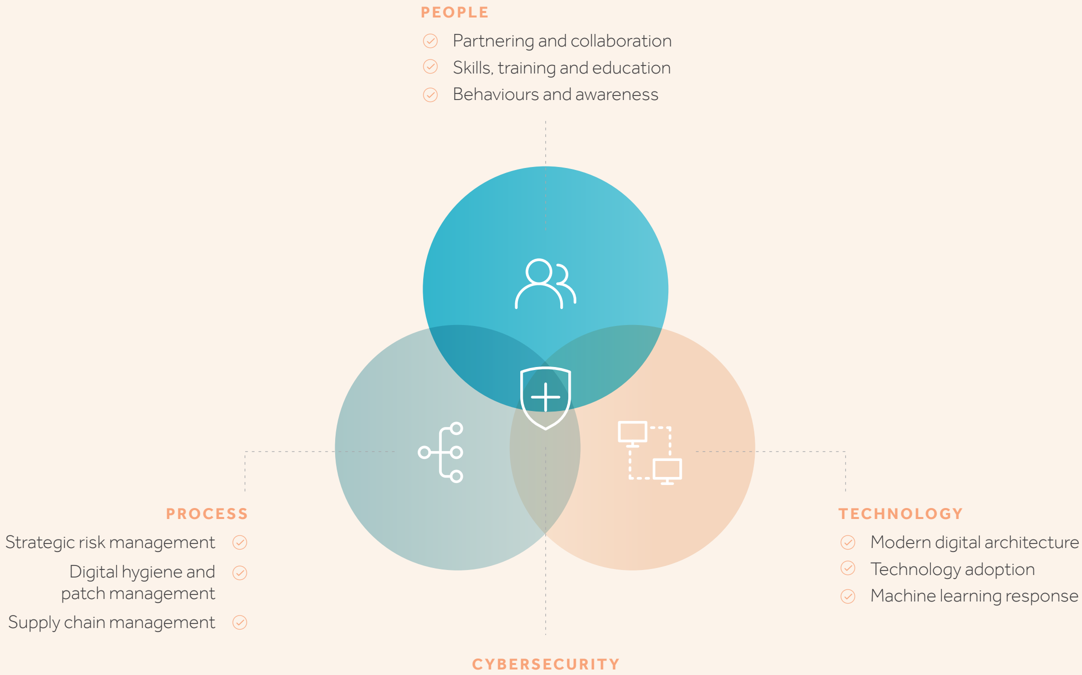
Mining plays an interesting role in the global economy; it is central to the development of all advanced economies but relatively few people have actually visited a mine site. Most governments consider mining assets to be critical infrastructure yet over half of the industry believes its approach to cybersecurity is immature or non-existent. In an environment of rapidly increasing digitisation, global interconnectivity and heightened cybersecurity risk and awareness, this perceived immaturity is likely to be short-lived.

Globally, industries are rapidly adopting new digital technologies in the pursuit of transformational productivity and competitive advantage. In itself, this transformation is a large undertaking requiring new investment, new styles of leadership and new skills. Digital architectures are moving from legacy, layered internal designs to flatter, integrated cloud systems – the implications of which are a host of new value opportunities for both businesses and their adversaries. Crucially, as digital systems become more powerful and integrated so does the potential value loss from successful cyber-attacks.

Mining adds the complexities of remoteness, potentially hazardous sites, global supply chains and increasing physical automation. So, while other industries and governments focus on the privacy and direct financial risks of cybersecurity, mining and natural resource industries must also focus on the immediate health, safety and environmental risks of cybersecurity.

FIGURE 01

PEOPLE, PROCESS, TECHNOLOGY – SAME SAME, BUT DIFFERENT


PEOPLE
✓ Partnering and collaboration
✓ Skills, training and education
✓ Behaviours and awareness
PROCESS
Strategic risk management ✓
Digital hygiene and patch management ✓
Supply chain management ✓
TECHNOLOGY
✓ Modern digital architecture
✓ Technology adoption
✓ Machine learning response
CYBERSECURITY

First and foremost, building cyber resilience is an added cost for miners. With this cost, however, comes a significant opportunity to use cybersecurity resilience to drive digital transformation and productivity in much the same way that the industry has benefited from automation and productivity in its quest to improve safety outcomes.

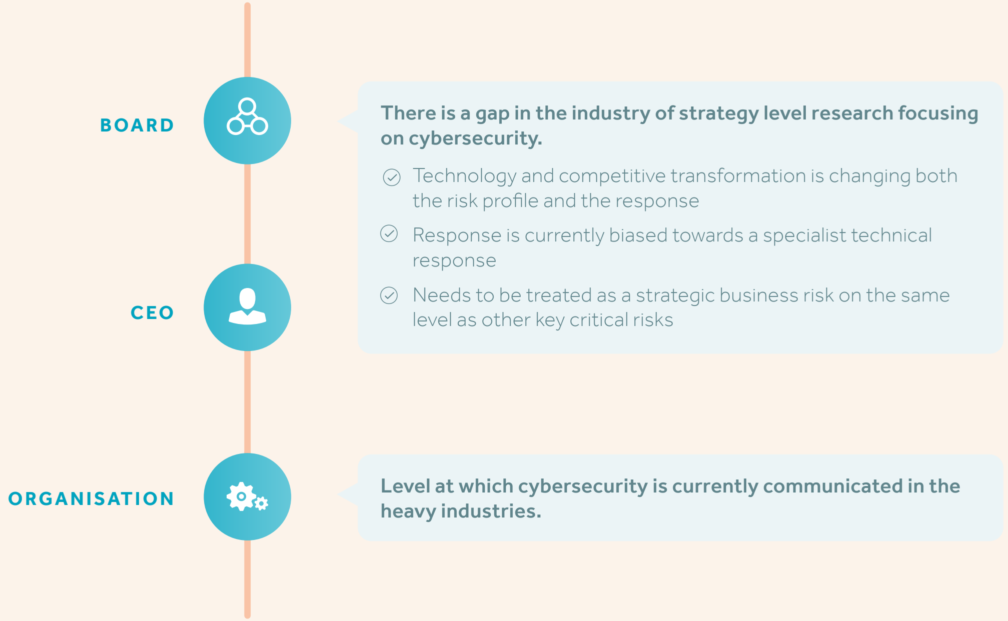
The overriding theme from our interviews with executives responsible for cybersecurity across the industry is that there is no silver bullet – managing cybersecurity can only be done at a strategic risk level. It is a multi-faceted challenge across people, process and technology. Across the following chapters, we will outline the major considerations and drivers for cybersecurity in mining and discuss emerging pathways forward.

Enjoy.

Graeme Stanway
Paul Mahoney
Kevin Ong

FIGURE 02

CYBERSECURITY IS CURRENTLY TREATED AS A TECHNICAL ISSUE, NOT A STRATEGIC ONE



There is a gap in the industry of strategy level research focusing on cybersecurity.

- ✓ Technology and competitive transformation is changing both the risk profile and the response
- ✓ Response is currently biased towards a specialist technical response
- ✓ Needs to be treated as a strategic business risk on the same level as other key critical risks

Level at which cybersecurity is currently communicated in the heavy industries.

CHAPTER ONE: THE STATE OF PLAY

It's All About Strategy

"I think that done properly it will be a competitive advantage for us."

With accelerating technology change, the disruption of incumbent business models is inevitable. The rapid rise in volume and success of start-ups, including 'unicorns', are an increasingly significant competitive force. Platform data service businesses are beginning to dominate across continents and industries and service businesses are shifting en-masse to subscription style business models. While many of these shifts are being felt in the mining industry, the industry has retained three main business models. In addition to the fundamental value drivers of safety and brand, each of these business models has its own distinct value proposition and implications for how cybersecurity risks manifest.

1. **Integrated supply chains: Disruption sensitive**
   e.g. large bulk operators in aluminium and iron ore
   Close relationships with key customers who value security of supply, low cost and product quality consistency. For these businesses, a major risk from cyber-attacks is the disruption of continuous production systems and its subsequent impact on their reputation for reliability with customers.

2. **Production for sale into liquid spot markets: Delay sensitive**
   e.g. precious metals operators in gold, silver and platinum
   Limited visibility of customers with minimal differentiation between products but are attractive to investors for their store of value. For these businesses, a major risk from cybersecurity is the disruption of their capacity to produce or trade at expected rates and its subsequent impact on the valuation of their assets by investors.

3. **Explorers and deal makers: Loss sensitive**
   e.g. junior explorers, traders and portfolio managers
   Value proposition is in securing previously unknown or undervalued mineralised assets. Historically, this has mostly been speculative but is increasingly in cooperation with end-customers with specific requirements. For these businesses, a major risk from cybersecurity is the theft of commercial and geological intellectual property from which they derive their competitive value and differentiation.

FIGURE 03

WE ASKED: DO YOU PERCEIVE ANY BENEFITS OTHER THAN THREAT MITIGATION ARISING FROM IMPROVED APPROACH TO CYBERSECURITY?

By % of respondents given two options

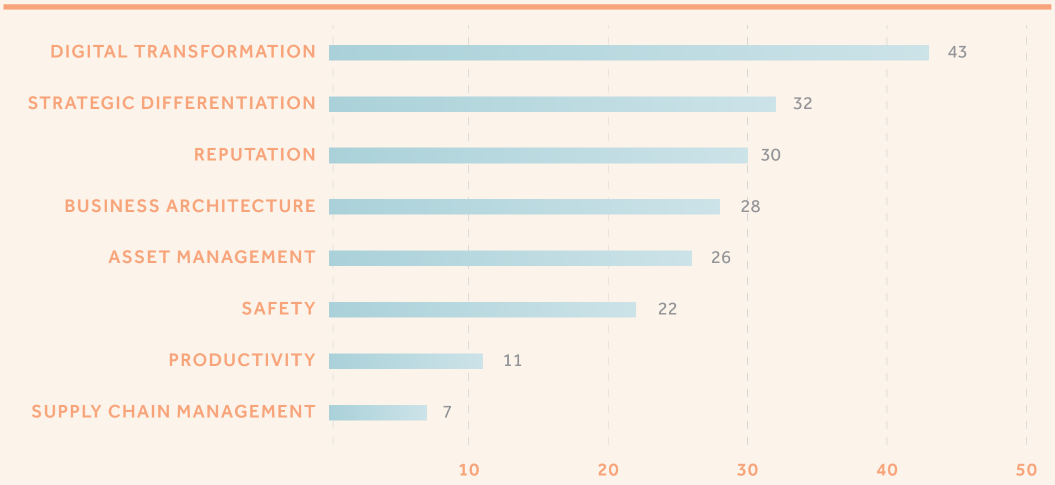
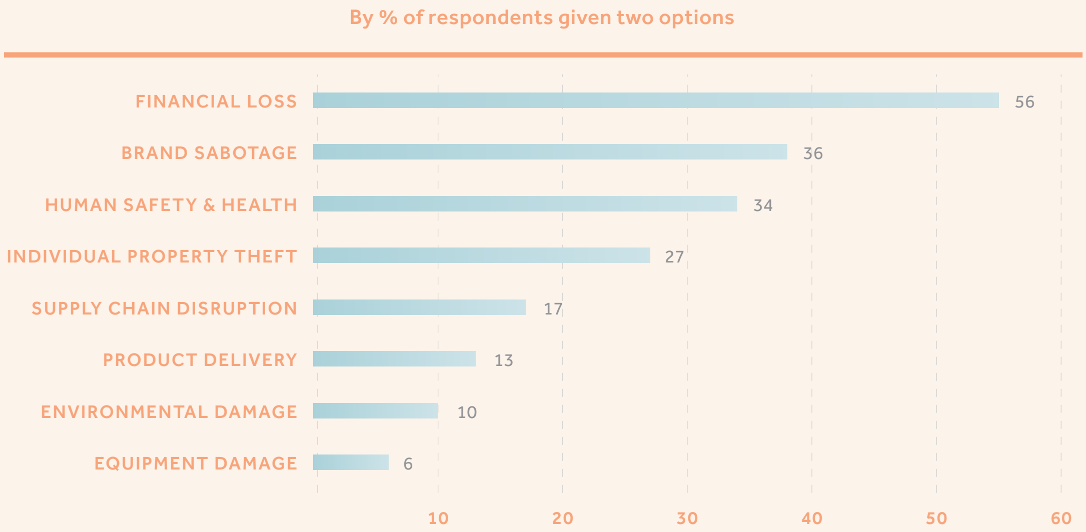


FIGURE 04

WE ASKED: WHAT ARE THE MOST IMPACTFUL CONSEQUENCES FROM CYBERSECURITY RISK FOR YOUR COMPANY?



Many of these companies are major sources of export revenue for their local governments, both directly and through the surrounding equipment, technology and services sector, providing an additional layer of strategic risk and complexity. As major cyclones and operating interruptions (including tailings collapses, safety incidents, union activity) across key mining countries like Brazil, Chile, South Africa, Australia, Indonesia and Canada demonstrate, ongoing interruptions to mining activities are felt in federal budgets. As such, pressure to achieve and maintain resilience to cyber threats is an ongoing reality for executives and may be leveraged for government support.

> "Cyber investment is good for business, we see it as an emerging competitive advantage as a base supplier for most supply chains."

Cybersecurity discussion and commentary can tend towards pessimism rather than positivity. A fascinating theme running through the executive interviews and survey data, however, is the enormous potential that cybersecurity offers to drive a broad range of non-security benefits. Some are profound – transformation, differentiation, productivity and safety – while others are more prosaic – asset and supply chain management.

Arguably the greatest commercial business threat is not financial loss, but loss of time – 'time is money and loss of time cannot be recovered.'

Digital transformation is the catchphrase of the 2010s, overused to the point of distraction – 'we have been doing digital transformation since the IBM PC hit the streets.' Despite all the attention it attracts, few large incumbent operating businesses have successfully navigated the process of wholesale digitisation. Common problems of cultural resistance, legacy architectures, over-emphasis on inflexible platforms and ill-suited governance processes have proved difficult to overcome for most. What these types of businesses are good at, including miners, is the mobilisation of processes and people to address key risks – paramount in these is safety.

Should companies be able to internalise the importance of cybersecurity and apply their strong historical cultures of risk management, there is a good chance that they will begin to gain some traction in the establishment of a modern digital architecture for their organisation.

Unique Mining Environment

"Control of mine sites is still done manually as the perceived cybersecurity risk of the internet of things is too high."

Mining businesses share large amounts of organisational DNA with businesses from other industries – financial systems, human resources systems, procurement systems, desktop systems, and many others – are much the same. In other crucial ways though, mining is a very different industry. It is facing several technology challenges alone and will ultimately be compelled to take leadership in these areas.

First among these is the challenge of geology. Unlike the natural gas or petroleum industries, geology is very difficult to characterise from a small number of samples. Natural history is highly variable and often unique to a given geography. Currently, mining companies design their value chains to absorb ranges of variability in the ore body, leaving much potential scope for improvement of production. Advanced ore characterisation through machine learning and operational responsiveness through automation of extraction and processing has the potential to create a huge lift in the utilisation of ore bodies and the inputs consumed. Assets will become, in effect, operated by advanced software. The embedded strategic cyber risks for mining businesses from this shift are clear.

A second major challenge is the remoteness of major mining assets. The pre-eminence of acquiring ore bodies in building business value means miners have limited discretion on where their assets are located. Many embed a sovereign risk layer to their investment decisions. It is difficult to avoid the issue of remoteness – just consider Australia's north-west iron ore basin or Canada's mining operations in the Arctic. Geography has influenced how security has traditionally been considered, leading to isolationist ('air gapped') strategies, made possible by the lack of interconnectivity to urban grids and networks. Automation and communications connectivity have made

FIGURE 05

WE ASKED: DOES YOUR COMPANY PLACE SUFFICIENT EMPHASIS ON CYBERSECURITY?"

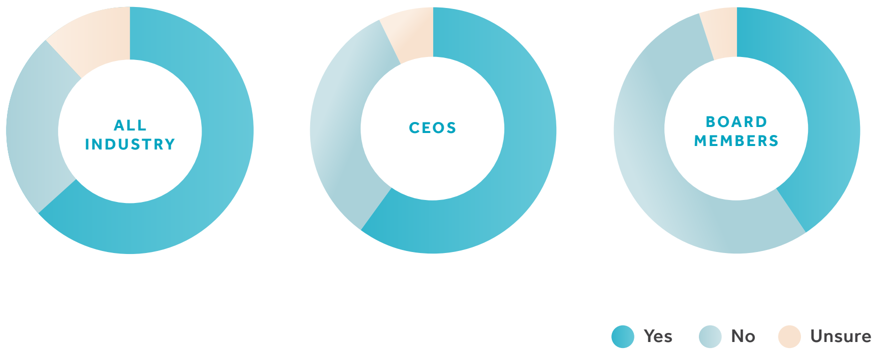
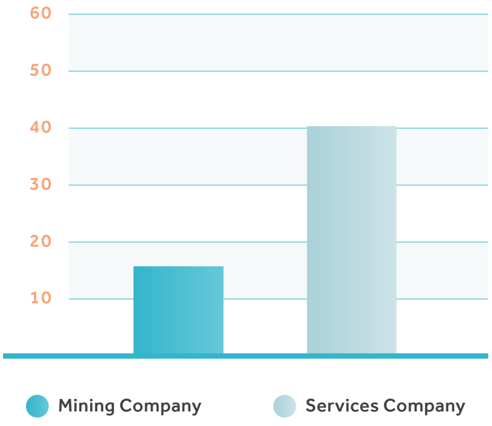


FIGURE 06

WHAT SORT OF COMPANY DO YOU WORK FOR? DOES YOUR COMPANY EVALUATE THE CYBERSECURITY PERFORMANCE OF SUPPLIERS?

By % of respondents who responded 'always'



this concept redundant, potentially causing a more abrupt shift for miners than for other, less remote, industries. Paradoxically, remoteness is the central driver for remote operations and autonomy.

A third challenge facing the industry that separates it from most industries are its long global supply chains and the number of specialist service companies brought to bear on extracting and delivering mining products. For this reason, suppliers are one of the main sources of cyber risk for mining companies and accordingly will need to become one of their main sources of cyber resilience. They are part of your overall enterprise and 'should be treated as such'. Unfortunately, the evaluation and testing of suppliers are 'currently poor across the board' which 'needs to be fixed now...there is a tsunami of technology in cyber-attacks that even the NSA cannot handle.'

Service companies are culturally far more responsive to their customers than mining companies because they have to be. As miners begin to prioritise cybersecurity in their commercial terms and communications to the market, suppliers will respond. The shift is already underway – of our survey respondents, over two thirds said a strong cybersecurity reputation will become critical for suppliers in the next five years. Another third said it will be important. None said it will be unimportant. Government bodies, in particular, recognise the global competitive advantage that advanced cyber capability will deliver their mining services businesses.

"With the next generation of satellites, no one will be remote and with the cloud, your data and applications could be anywhere in the world, including at the bottom of the ocean."

FIGURE 07

CYBERSECURITY ACROSS TIME

	PHYSICAL CONTROL (Pre-digital)	DATA CONTROL (Purdue)	FLUID CONTROL (Future)
THE GAME	Security of known, static locations of value	Layers of digital security & access control	Artificial intelligence 'arms race'
ENABLERS	✓ Physical stores of value ✓ Known locations ✓ Little traceability once stolen	Technology change ✓ Digitisation of global business ✓ Patch management ✓ White collar workers	Technology change ✓ Global (fast) internet ✓ AI & machine learning power ✓ Automation and IoT

THEN NOW FUTURE

Shift to Modern Digital Architectures

Conservatism with respect to production-based technology adoption has been a hallmark of mining companies for a long-time. In an industry inherently exposed to high levels of human safety risk, environmental risk and market risk, adding the seemingly discretionary risk of technology had long been considered cavalier. Over the past decade in which we have been surveying the global mining industry, we have witnessed a significant shift in this mindset, from a majority of self-described 'fast followers' to 'industry leaders'.

"Most mining companies have legacy infrastructure in place that both poses high security risk as well as being an impediment to the adoption of new technologies."

The legacy remains, however. As is the case for many high-risk industries, a surprisingly large number of core operational technology systems are married to extremely out-dated applications. This is as true for the space and airline industries as it is for mining. Simply put, the risk of making changes (with all their poorly understood flow-on effects) can be deemed too great.

"Security is a terrible word; it makes you think there is safety in a big door. But in reality, there are a million little holes and you just need to find one and then you're in."

Complexity is becoming unmanageable as such legacy systems become intertwined with technologies due to the sheer rate of adoption, both planned and unplanned. Historically, software was purchased at very senior levels and licensed to all users in large commercial deals. Whilst this still happens with cloud platforms and ERP systems (to name just two), there is an increasing trend towards users having the discretion to subscribe to software themselves. It is this sales model that has catapulted start-ups such as Atlassian to market capitalisations in the tens of billions of dollars. It is also underpinned by organisational innovation and cultural initiatives.

The Greenfields Design Opportunity

The mining industry today is more exposed to cybersecurity risks than ever. As miners push forward into new territory with the integration of new technologies into their operations, their attack surface increases and with it their overall cyber risk.

Survey feature: Top 3 technology trends identified as having the biggest impact on cybersecurity over the next 10 years:

1. Artificial intelligence and analytics (87%)
2. Sensing and data (60%)
3. Robotics and automation (45%)

Greenfield mining operations offer significant opportunities for implementing robust and flexible cybersecurity systems well equipped for the supply chain of the future. The benefits of building-in and maintaining cyber systems at an early stage are numerous: they are more effective, less costly long-term and can enable future business.

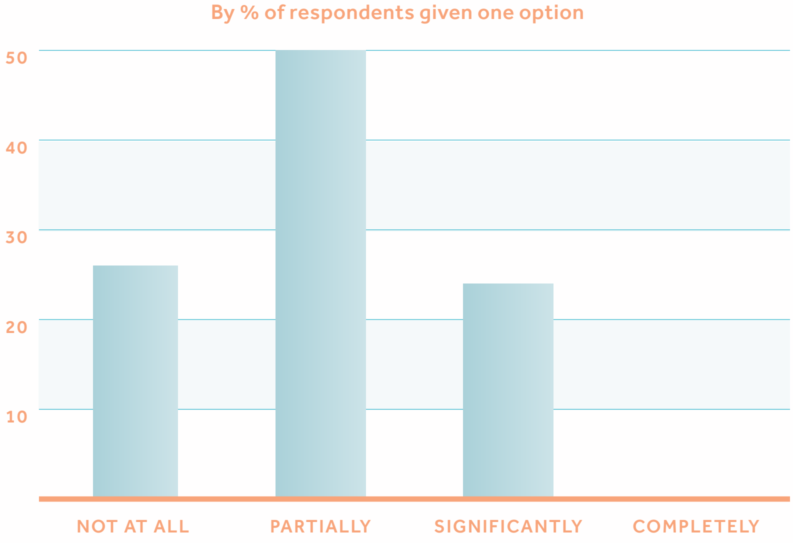
The major challenges in designing cybersecurity systems for greenfield operations are:

- Building in flexibility to cope with current and future plug-in technologies; and
- Managing risk exposure brought by equipment and sensors, and by 3rd parties.

Major priorities are therefore developing cybersecurity systems that are secure by design and are based on a trusted ecosystem. New mines leading the way in technology integration – for example, Syama and Borden – can act as a testing ground for this approach.

FIGURE 08

WE ASKED: TO WHAT EXTENT IS CYBERSECURITY THINKING INTEGRATED INTO MINING ASSET DESIGN AND OPERATION?



“You have to remember you spent millions getting systems up for a reason, the major problem is that these are based on the assumption that everything will go as expected.”

Alongside new software is the exponential growth in connected devices on mining networks due to investments in automation and monitoring. Unlike much legacy technology on mine sites, these sensors and actuators have relatively short expected lives (both through technology obsolescence and reliability), creating ‘bow waves’ of sustaining capital expenses, depreciation and asset management complexity. With this increased automation and integration, ‘air gapping to contain and isolate cybersecurity attacks...is no longer an option and is ineffective.’

For cybersecurity teams, the complexity created through the melding of new technology with legacy systems is a double-edged sword. In one respect, the complexity has created a broad playing field for cyber adversaries to find and exploit vulnerabilities. In another respect however, it has also created a layered defensive arrangement that in some cases may complicate the speed and breadth of attacks. On balance, complexity with all of its technical debt is considered to be undesirable by cyber professionals in any industry – and things will get worse until newly adapted security processes and protocols are in place. As one interviewee put it, ‘a secure system is a simple, well-maintained system.’

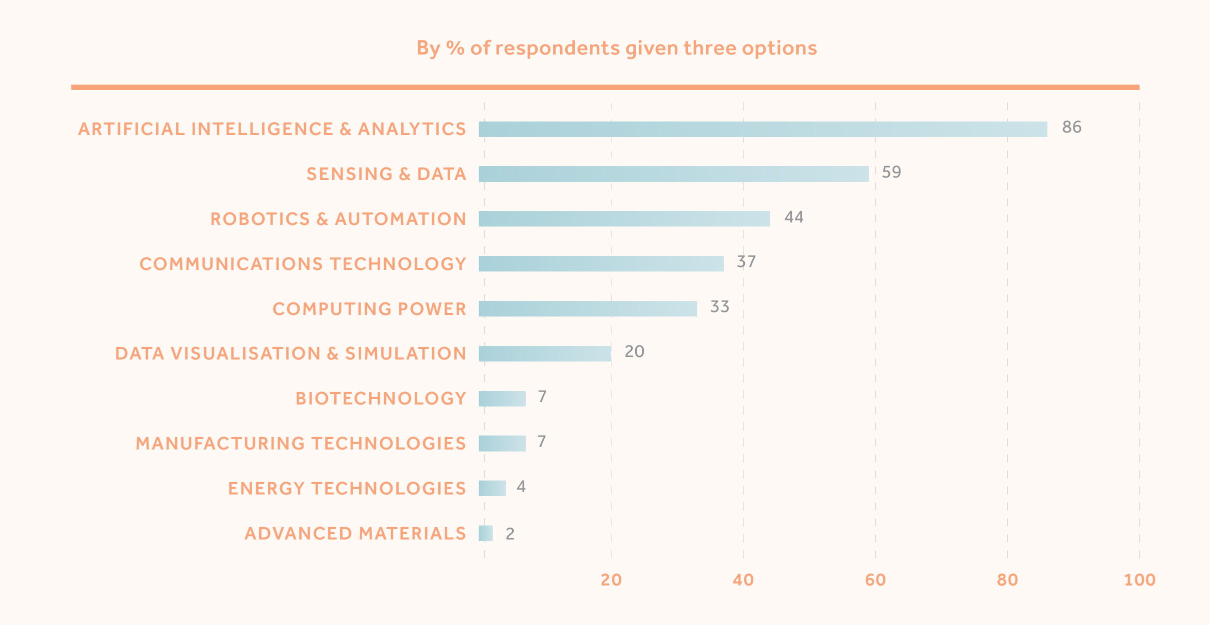
Simplicity of systems and architecture design is going to go a long way towards solving many of these issues. In fact, building cyber resilience will itself give impetus to a shift in architecture that is simplified, standardised and more efficient. Lifting cyber as a priority in the design of these systems is highly aligned with the objectives of digital capability and systems performance in general – modular, upgradeable, testable and integrated. Quite the contrary from being the ‘handbrake’ to digital transformation that cybersecurity is commonly considered to be.

A major implication of these shifts is the move to cloud-based data and software systems. One interviewee with deep technical expertise explained that this will reduce the number of security layers ‘from nine to one’. Modern architectures also imply different possibilities for how cyber software is deployed – edge computing offers the opportunity to decentralise defence software and protect data and commands before they are transmitted. Another pathway unlocked by this shift is the capacity to utilise the computing power available on large cloud data servers to use simulation to foresee and act proactively to potential catastrophic risks. This offers the tantalising possibility of breaking the very real catastrophe to regulation cycle.

It also offers the opportunity to outsource large parts of the security task to global behemoths whose core value proposition relies on securing their client’s data – these businesses include Microsoft and Amazon, with their thousands of cybersecurity professionals. As a relatively small part of the revenue of these businesses, however, the imperative to address mining’s specialist security needs will always be marginal. In addition, like aircraft carriers, they are well protected for a reason; ‘did you know that cloud customers were hit with over six hundred million cyber-attacks last year?’ As several interviewees reiterated, every business ultimately owns its own risk – it cannot be outsourced.

FIGURE 09

WE ASKED: WHAT TECHNOLOGY TRENDS DO YOU BELIEVE WILL HAVE THE BIGGEST IMPACT ON CYBERSECURITY OVER THE NEXT 10 YEARS?



What we are likely to see, because of the above requirements and advantages, is the growth of integrated services that excel in the design of integrated cyber resilient systems and software. In the companies that provide these services, skills in cyber, machine learning and user-centred design will come together. Businesses such as Singtel, Google and Palantir are at the vanguard of this movement. Prioritising users is critical for cyber, and indeed for success in digital transformation, enabling people to engage and do the right things intuitively. The best start-ups understand this viscerally.

> "There must be transparency in systems put in place as well as a deep understanding of how their roles interact."

Two Types of People Problem

"There is and always will be a behavioural aspect – the attacker is a person or group with their own ideals, objectives and motivations. They will use tech, so we need to counter with tech."

Cybersecurity is a people problem in two very distinct dimensions: the adversaries actively attacking and the users within companies and suppliers whose behaviours create opportunities for attack. Both problems are fundamental; 'you can't take people out of the equation'. Adversaries are people and will always adapt as technology improves, while the behavioural problem of users will continually evolve with the ingenuity of attackers.

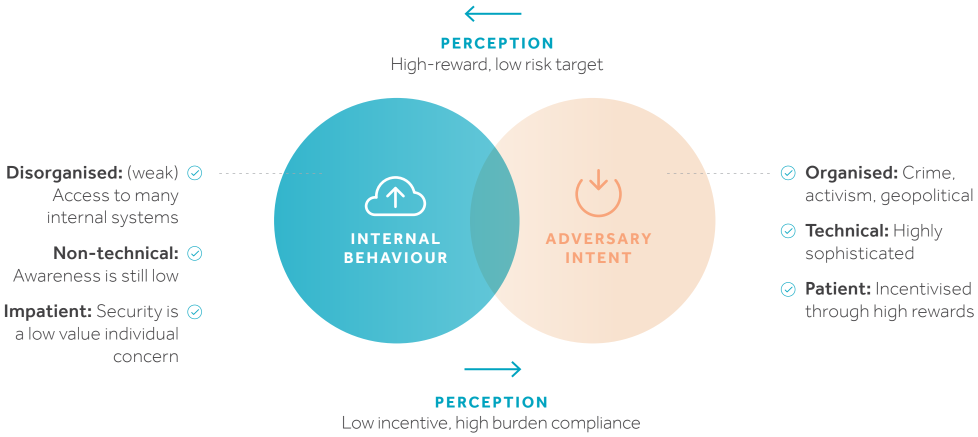
Today, security is 'like the Maginot Line' with static control points and the reality is that the cloud 'is going to pave the road around our old defences.' In this environment, defence will need to shift to adaptive diagnostics and fluid control points based on the extensive application of machine learning. Whether attackers will always have the upper hand – 'machine learning and other forms of artificial intelligence are much more useful for attack than for defence' – is debatable – 'the notion that artificial intelligence is more powerful for attackers is not true and is in fact a dangerous generalisation'. The ongoing arms race is why large technology providers are mobilising, seeing in this ongoing conflict an enormous long-term economic opportunity.

The primary reason is that the game is ultimately zero sum – cybersecurity teams have to use technology to protect themselves at the speed in which they are being attacked. It is difficult to get ahead of the game. Technology in this respect 'cannot save us', as it is a people problem. Believing that artificial intelligence or machine learning alone can win the war is incorrect – hackers excel at applying creativity and novelty in how they attack. By definition, hackers are creating the very edge cases with which artificial intelligence and machine learning, based as they are on patterning historical data, are bad at identifying. Once identified, these tools are fantastic at responding but the initiative will always be with the attacker.

An effective defence will require the application of such technologies combined with a good understanding of who the adversary is and their motivations, providing 'some indication of where the deployment of technology needs to be'. The development of capability to support these defences requires internal and external cross-functional skill sets across operations, cyber and commercial partners. Making mining systems more secure can also be a function of making itself less attractive as a target – that is, frustrating strategies attackers use to make money. A simple example is maintaining ample back-up to reduce the possibility of being denied use of your own data in a ransomware attack, thus reducing the requirement to pay a ransom.

FIGURE 10

"TWO TYPES OF PEOPLE PROBLEM"


PERCEPTION
High-reward, low risk target
Disorganised: (weak) Access to many internal systems
Non-technical: Awareness is still low
Impatient: Security is a low value individual concern
INTERNAL BEHAVIOUR
ADVERSARY INTENT
Organised: Crime, activism, geopolitical
Technical: Highly sophisticated
Patient: Incentivised through high rewards
PERCEPTION
Low incentive, high burden compliance

The Cyber Start-up Scene

The evolution of cyberthreats and the diversity of attacks are paving the way for more security solutions. Cybersecurity product sales are predicted to reach $124 billion in 2019, up from $114 billion in 2018.[1] Unsurprisingly, this pool has given rise to a massive ecosystem of security start-ups. A significant barrier faced by start-ups, particularly in Australia, is the reluctance for venture capital funds and companies to invest in early-stage cybersecurity technologies. Instead, they prefer to wait until there is evidence of customer and revenue growth, which can take longer to develop in the cyber industry. Mining companies should look to leverage Australia's capabilities in software and cyber services by partnering and investing in early-stage cyber tech start-ups.

Cybersecurity capability also forms a fundamental piece of the puzzle for mining equipment, technology and services start-ups. Integration of cyber-secure practices into product development represents a global strategic opportunity and will be required to build a competitive position in the global market.

Although mining company evaluations today are dominantly ad hoc (42%), one-off (13%) or never (6%), companies that consider their cybersecurity strategy highly successful carry out supplier cybersecurity evaluations quarterly. This level of scrutiny speaks to the future of procurement in the mining industry and the level of regulation required moving forward.

FIGURE 11

WE ASKED: HOW IMPORTANT WILL A STRONG CYBERSECURITY REPUTATION BECOME FOR EQUIPMENT AND SERVICE COMPANIES OVER THE NEXT 5 YEARS?

By % of respondents given one option

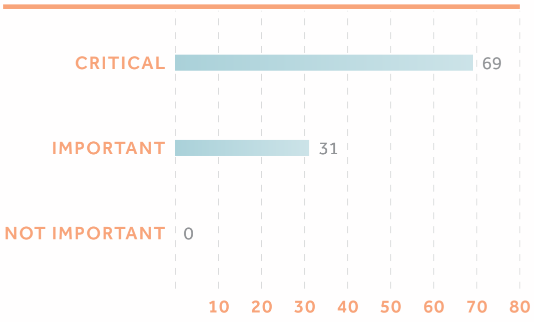
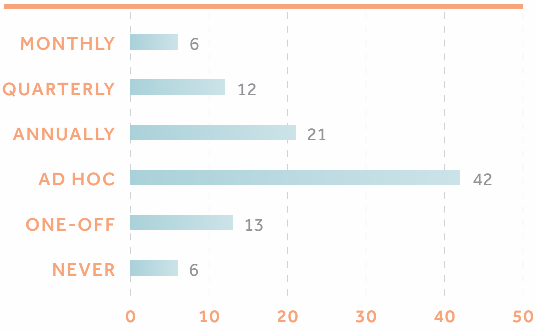


FIGURE 12

WE ASKED: HOW REGULAR ARE YOUR CYBERSECURITY EVALUATIONS FOR A GIVEN SUPPLIER?

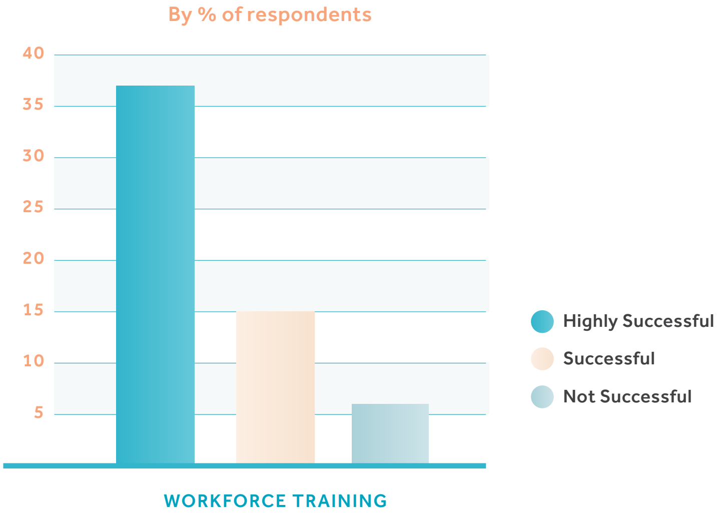
By % of respondents given one option



[1] Forbes 2019: Top 10 Cybersecurity Companies to Watch in 2019

FIGURE 13

WHAT INTERNAL LEVERS DO YOU BELIEVE WILL IMPROVE YOUR BUSINESS' CYBERSECURITY RISK MANAGEMENT? & HOW SUCCESSFUL DO YOU BELIEVE YOUR COMPANY'S CYBERSECURITY APPROACH HAS BEEN?



In the current environment, the workforce is easy prey for adversaries. Many of our discussions leant on the issue of behaviours and users being the source of vulnerabilities, with the implication that it is naïve to believe that awareness and education will ever eradicate this issue. Even in workplaces with the most direct impact on health and safety – hospitals – it is extremely difficult to maintain high performance of the most basic necessity, bacterial control through the act of washing hands. League tables of hospitals show that at best, an individual hospital can maintain high rankings for only a few years while senior staff place a priority on it – with success, however, comes complacency and the subsequent rise in infections.

How many of Microsoft Excel's almost five hundred functions have you used? This is the zone of ignorance – most people learn to use computers 'flying by the seat of their pants'. Even if they have taken courses, it is difficult to remember most of what they've learned – 'thirty percent of people in the workforce don't even know that you can have two windows open at the same time.' People are at best basic novices in using computers so the very notion of asking them to behave properly is a questionable strategy, even if done well. Despite this, mining has had some success in changing broad-based workplace behaviours in the past.

"People are often the core reason for cyber-attacks, they are the ones that are leaving holes...which open up systems for attacks."

Safety in the mining industry was very poor until the 1990s and early 2000s when communities and executives could no longer accept the impact on human life of mining activities. Across the industry, behavioural programs had great success in decreasing safety incidents. In the past decade, however, improvements have plateaued as the industry faces the limits of behavioural risk reduction. From here, it needs to be designed out through automation. While we expect cybersecurity to track a similar path, it is still unclear to most how the risk can be designed out.

Several executives highlighted the good design of user interfaces and subliminal techniques such as nudge methods to circumvent the worst habits of people. In order to succeed with this strategy, concerted and deliberate engagement and co-design with suppliers is necessary. Corporate systems are notoriously difficult and clunky to use, much can be improved through 'a simplification of the user experience to ensure that cybersecurity controls are consistently used without hindering the efficiency of the user.'

Governance & Strategic Risk Management

> “Cybersecurity needs to be approached through a strategic risk management process with the identification and prioritisation of known threats and vulnerabilities.”

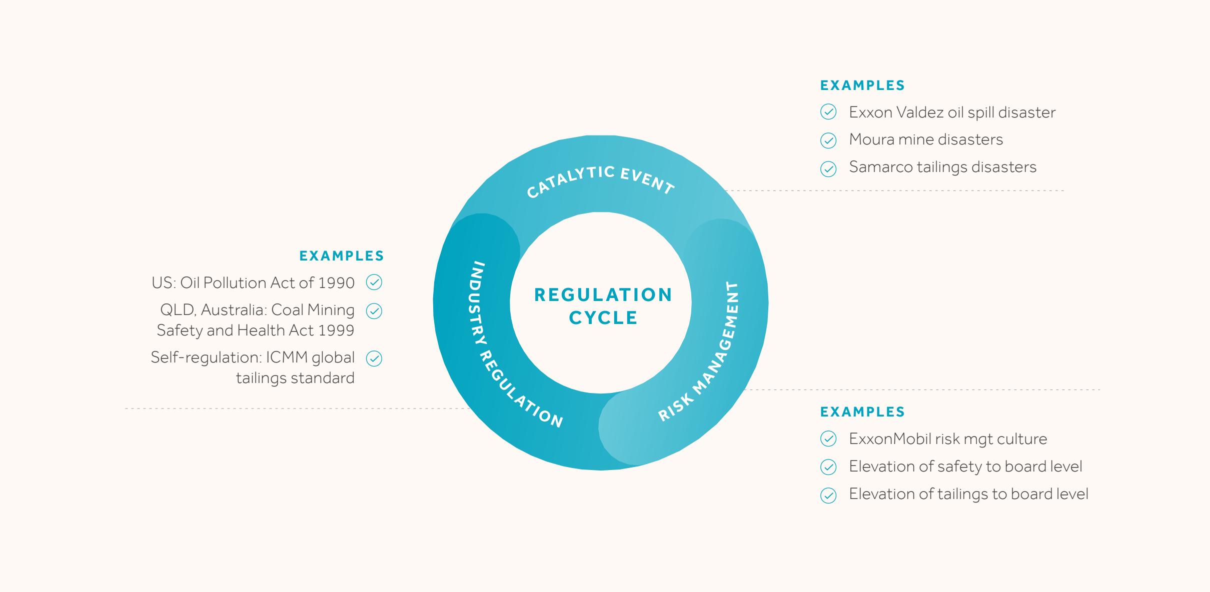
Perhaps surprisingly, the interviews revealed that chief information security officer roles focus more on people and processes than on the technical aspects of cybersecurity. Risk management is being applied as the vehicle for managing cybersecurity across these large, well-run natural resource businesses. It is considered highly useful because of the complex and dynamic nature of the cyber challenge combined with the natural affinity and competence with it as a methodology. Cybersecurity lends itself to a risk-based prioritisation and mitigation process, in the same way that other strategic risk areas are managed such as safety, environment and market risks. As a high-risk endeavour with a highly risk conscious temperament, mining's capability and culture is extremely well adapted to managing issues in this way.

Cybersecurity is different from other strategic risks in one important dimension – adversaries are dynamic and incentivised to adapt. Adaptation at this rate is not the case for other major risks like safety and environmental risks. As such, and despite the good initial fit, risk management methodologies can't be adopted for cybersecurity without adaptation. Attackers can 'change the incentives, and hence behaviours, of the defenders.' The reverse is also true. This kind of thinking 'opens up novel mitigation strategies beyond the traditional risk management thinking.' A salient example of this is the effectiveness of an entire industry banding together to refuse to pay ransoms from ransomware, thus 'reducing the incentives of the attackers to attack in the first place.'

Technology may come to be a key tool for risk management more broadly, the ability to apply analytics for soft sensing and detection of issues or to virtually simulate operational scenarios (to pre-empt occurrences) is accelerating quickly. Strategic risks, such as cybersecurity, have always posed a general challenge of low probability, high consequence events – lending itself to the application of such simulation principles.

FIGURE 14

THE REGULATION CYCLE



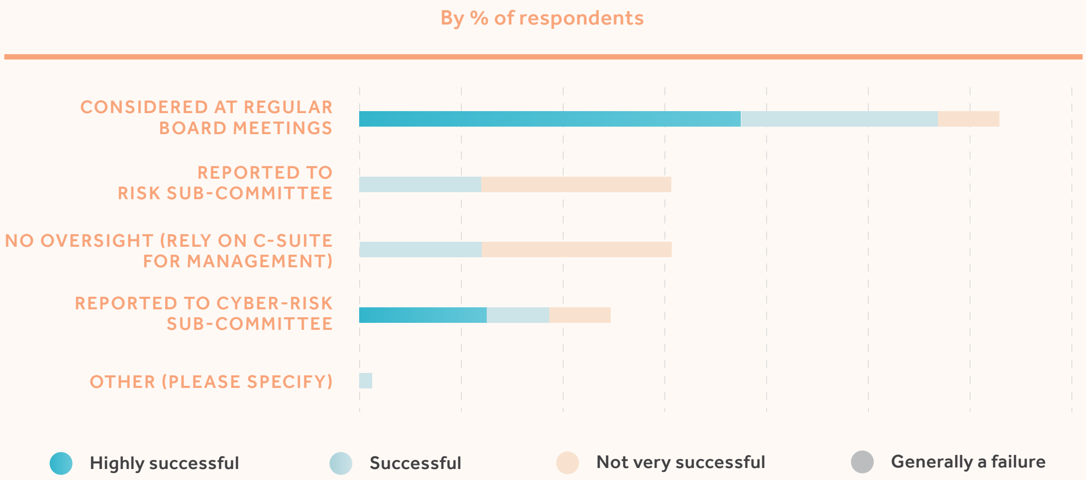
EXAMPLES
- Exxon Valdez oil spill disaster
- Moura mine disasters
- Samarco tailings disasters

EXAMPLES
- US: Oil Pollution Act of 1990
- QLD, Australia: Coal Mining Safety and Health Act 1999
- Self-regulation: ICMM global tailings standard

EXAMPLES
- ExxonMobil risk mgt culture
- Elevation of safety to board level
- Elevation of tailings to board level

FIGURE 15

HOW SUCCESSFUL DO YOU BELIEVE YOUR COMPANY'S CYBERSECURITY APPROACH HAS BEEN?
& HOW DOES YOUR BOARD OF DIRECTORS MAINTAIN OVERSIGHT OF CYBER RISK?



> "Boards need to understand the implications of cybersecurity in the language of finance, reputation, competitive position and customer trust. They do not need technical knowledge as it changes too fast to be useful to them."

Cybersecurity has quickly vaulted up most lists of global or business strategic risks to the point that around three quarters of all mining companies provide some level of oversight of cyber risks at the board level. This is sensible and desirable as boards form a crucial piece of the puzzle in forming a response to cyber risks – notably, among all respondents, board members are most aware of cybersecurity issues. Despite this awareness and prioritisation, 'boards today are poorly equipped to meet cybersecurity challenges; they do not have the experience or worldview necessary as problems in this era become increasingly digital.'

Boards must be able to filter technical advice from their security executives in order to make judgements on strategic implications and prioritisation. This is the perennial issue for all strategic risks; they are always technically complex. Mining boards have been

chastened by recent events such as tailings dam failures, environmental impacts, exposure to terrorism and geopolitical volatility among major trading partners – getting strategic risk management methodologies in place is at the top of their agenda. They see deficiencies in approaches to strategic risk management across the board and are searching for mechanisms to improve.

Borrow & Lead

> "Some things can be borrowed from consumer autonomous vehicles, but not as much as you think."

It is true that many aspects of mining are unique to the industry, but this does not mean that everything else isn't applicable – 'a corporate network is a corporate network.' With the possible exception of autonomous mining vehicles and automated processing plants, much can be borrowed from other leading industries in building responses to cyber threats. As over half of our survey respondents said, mining is an immature industry with respect to cybersecurity so the question is – who will come out and lead? Will it be big miners, big existing software companies or perhaps innovation from smaller businesses?

In reality, and despite the degree of talent and investment, 'it probably won't be Silicon Valley'. The reason for this is that the mantra that has underpinned so much of their success is diametrically opposed to creating cyber secure applications. This mantra is to release software updates as quickly as possible, in the full knowledge that there are flaws, and rely heavily upon users to tell them where the bugs are. Businesses such as Microsoft and Adobe 'institutionalised this'.

Cybercriminals 'love this, they know they can bank on there being vulnerabilities.' Cybersecurity teams are constantly taking one step forward and two steps back. All mining companies have adopted one operating system or another – 'these are massive elephants, and we're stuck with them' – and have to rely upon highly responsive patch management strategies. As such a small revenue stream for operating system and cloud providers, mining companies should not expect much effort in technical areas specific to the industry.

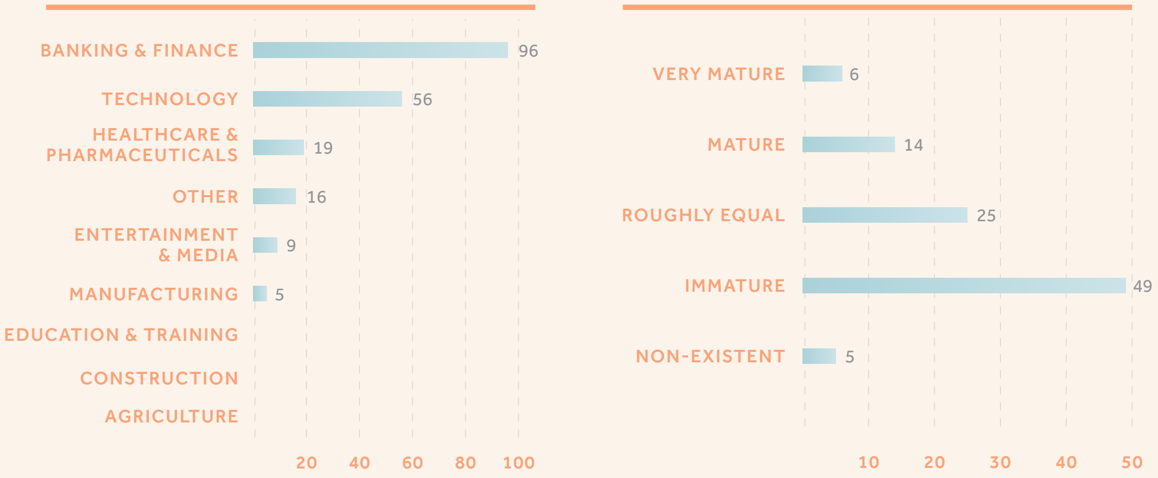
FIGURE 16

WE ASKED: WHICH INDUSTRIES DO YOU BELIEVE ARE THE MOST MATURE IN THEIR APPROACH TO CYBERSECURITY?

By % of respondents given two options

WE ASKED: HOW MATURE DO YOU BELIEVE THE MINING SECTOR'S APPROACH TO CYBERSECURITY IS RELATIVE TO OTHER INDUSTRIES?

By % of respondents given one option



Unless, that is, they are able to create organisations or industry groups that define the level of risk they will tolerate before they buy. Before 'we take the next big step, we need to figure out how to take control'.

There are huge incentives to take this next big step. Several countries around the world benefit from mining being one of their largest two or three industries, upon which they rely for their overall macroeconomic health – they will be very interested in supporting leadership and technology adoption in this area. Opportunities for doing so abound, the question as always is who in the industry will take the lead. The current approach for cybersecurity in mining is generally based on ISA-95, which 'has worked well to date.'

> 'We will break all the cyber design assumptions with an internet-connected plant – I don't know how to secure it. Nobody does.'

Innovation is always driven by needs, so it is not unreasonable to expect the industry to innovate in the areas of uniqueness it has, where nobody else will. The alternative is an intolerable level of risk in key core process activities. For example, data relating to raw mining products, maintenance schedules of equipment or arrangements of the environmental discharge system may be tampered with without anyone realising. At the scale of operations in mining, not to mention other industries, small changes like this can create large flow on effects – it does not need to be enormous catastrophic events to be damaging. One thing is for sure, as we become more and more dependent on systems that are automated, watching the decisions of the industry unfold from here will be fascinating.

Collaboration to Shift the Industry

"Pull together some mining companies, automation companies and cyber companies and work out what the next mine operations security model looks like."

Mining has an inconsistent record when it comes to collaborating at an industry level to address major challenges. For every successful example like safety or, more recently, tailings, there are many other examples of major companies choosing to 'go it alone'. Cybersecurity complicates this even further. Despite being an indisputably important risk, general perceptions tend to associate cyber issues with poor management. Several of our interviewees even stated that cybersecurity is one of the few crimes for which 'victim blaming is acceptable'. It is also an area in which collaboration is 'limited by the nature of cybersecurity threats. It is often impossible to explain cybersecurity threats without providing in-depth information about the internal systems of companies.'

The industry will, however, benefit from 'adopting a herd mentality' to protect everyone from being hit by the same thing. Indications exist that 'green shoots of collaboration' are emerging. The Mining and Metals Information Sharing Analysis Centre (MM-ISAC) was created by a small number of mining companies in 2017 following a major cyber incident in one of the companies. It has since grown by over three times as other global mining companies have joined to improve their collective cyber security and resilience – 'collaboration amongst mining firms is going well. There isn't an objection to it, just no awareness of what the next step is.'

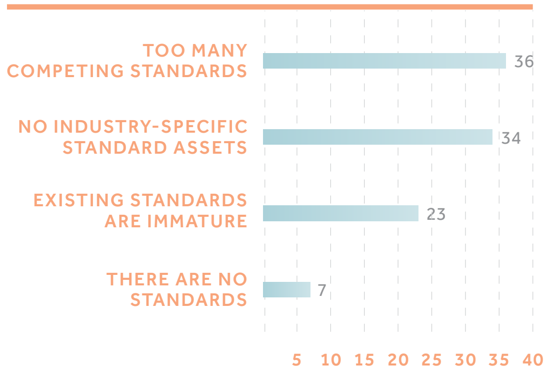
Depth and breadth of information and analysis is the big prize of industry collaboration in cybersecurity. By combining and scanning internet traffic flow through mining companies, a level of intelligence beyond even that of the National Security Agency has been achieved. No company can do this alone. MM-ISAC believes that the industry's collective approach 'will evolve over the years', but that they will identify which companies want to take a lead in this space and 'will help them work out the model for the industry.'

In Australia, over half of national export revenue comes from natural resources. Given this, government has identified the mining industry as the vanguard for a national, strategic response to the evolving cyber threat landscape. Through government-led industry bodies such as the Australian Cyber Security Centre and AustCyber, there is a concerted, collaborative and cross-sector effort to build industry resilience. A complimentary approach is being taken by METS Ignited, drawing on international capabilities through collaboration with Global Mining Guidelines to develop a set of industry standards across the Australian mining services sector. One final approach emphasised by a number of interviewees was the growth of operational test labs that mimic mining operations which may come to play a key part of an industry response and upskilling.

FIGURE 17

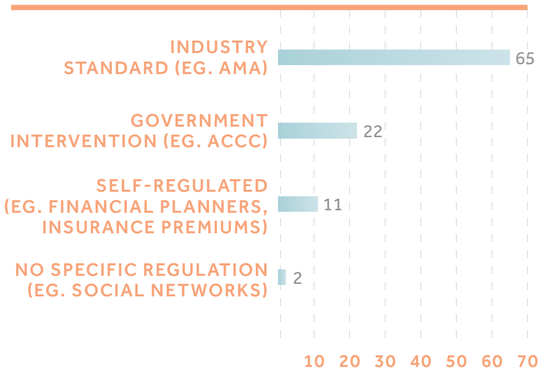
WE ASKED: WITH RESPECT TO CYBERSECURITY STANDARDS, WHAT DO YOU SEE AS THE GREATEST CHALLENGE?

By % of respondents given one option



WE ASKED: HOW SHOULD YOUR INDUSTRY BE REGULATED WITH RESPECT TO CYBERSECURITY IN THE FUTURE?

By % of respondents given one option



The transactional nature of the commercial relationships between mining companies and their suppliers is a broader issue that has big implications for collaboration in cybersecurity. Our broader industry survey on strategy and innovation lists this as one of the largest impediments to innovation in mining, and it will be no different here. However, there is a clear synergy in the incentives of miners and suppliers – mining companies are primarily concerned with managing risks and costs, whereas suppliers are concerned with building products and revenue. The risk imperative needs to be made clear for the mining equipment and technology service companies in how buying decisions will be made. Service companies will naturally respond – 'this is collaborative innovation 101'.

> "Waiting for a catastrophe to motivate change is like waiting for someone to shoot you to make your mother worry about your safety. We have to band together now."

Simplification, Standardisation & Supply Chains

"There needs to be a better relationship with third party vendors and ask real questions about who is responsible for what."

Fusion energy is considered the technology that is always twenty years away – perhaps wholesale industry collaboration in cybersecurity will ultimately remain 'a long way off' as well. Until it arrives, mining companies will need to take steps internally to improve their own security. The consistent philosophy driving many of the executives we interviewed was to focus on simplification, standardisation and the supply chain.

Simplification requires first understanding 'what we have' and then undertaking the modernisation and normalisation of legacy systems. In most instances this means taking 'a platform approach to how we consume our data.' A lot of analysis undertaken in the mining industry is still bespoke and located on individual devices rather than done through platforms. Given the rate of change of digital technology and innovation in small service companies, embedding scalable data and communications platforms and focusing on managing the standardisation of interfaces is central to an effective cyber strategy. Ultimately, this will enable executives to 'steer people away from shadow information technology systems and enable building controls around the interfaces.'

FIGURE 18

HOW SUCCESSFUL DO YOU BELIEVE YOUR COMPANY'S CYBERSECURITY APPROACH HAS BEEN? & WHICH OF THE FOLLOWING STATEMENTS BEST DESCRIBES YOUR ORGANISATION'S POLICIES REGARDING CYBERSECURITY?

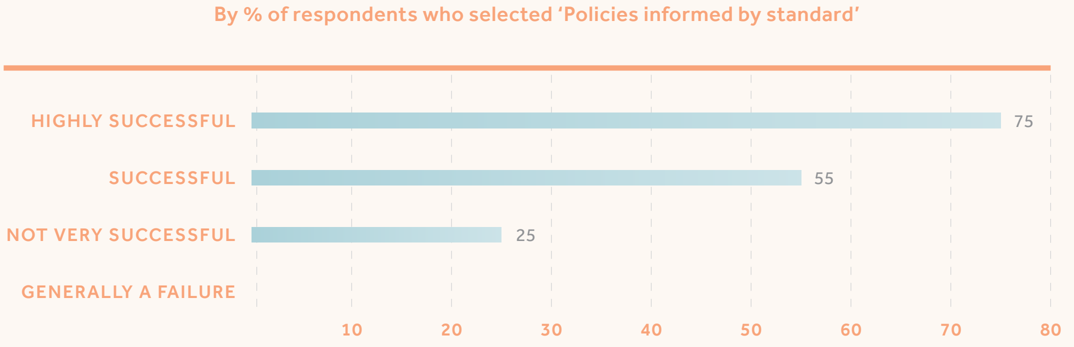
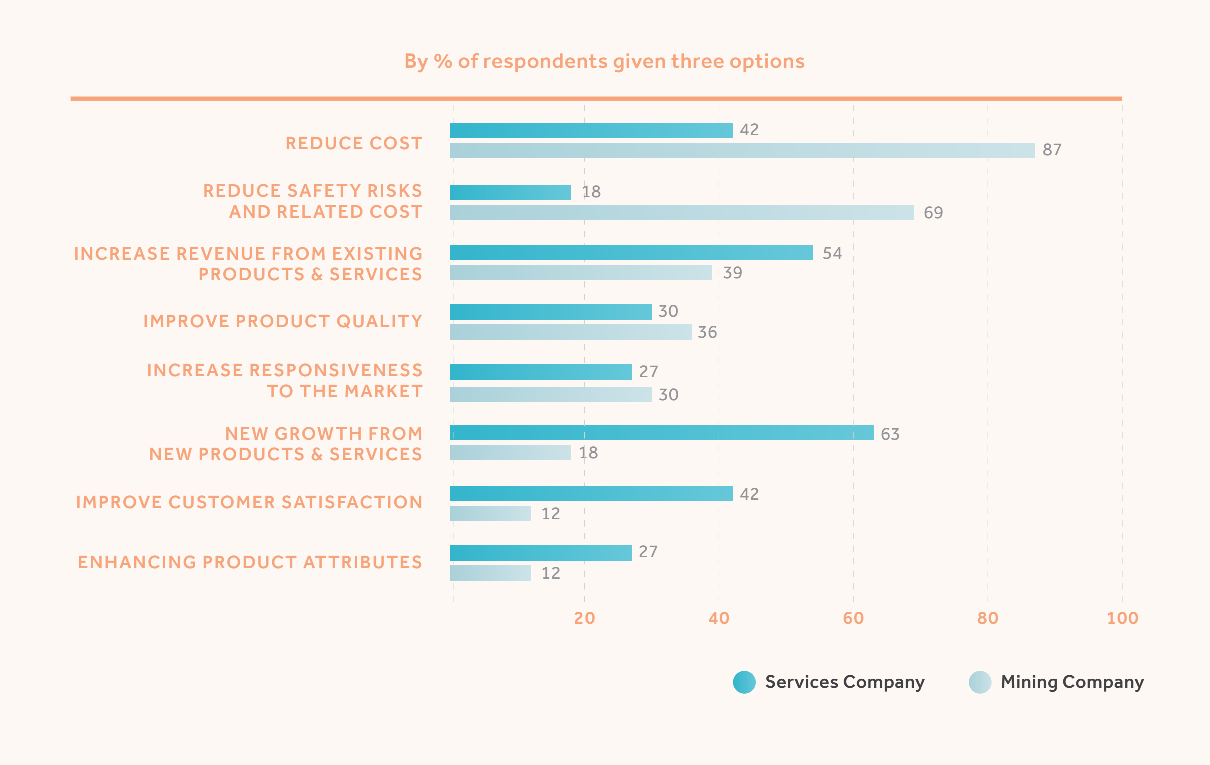


FIGURE 19

WE ASKED: HOW COULD DIGITAL TECHNOLOGIES CREATE BUSINESS VALUE FOR YOUR COMPANY OVER THE NEXT 5 YEARS?



Companies will need to invest in the definition or adoption of a level of standardisation to communicate with suppliers, specifically focusing on the standardisation of integration points between connected devices, data systems and software applications. The objective of doing so is to 'protect the data, codify the controls and codify the end user policy.' Interestingly, even within large companies, the importance of building pre-emptive cybersecurity controls into commercial agreements is often not well understood outside of security teams. One interviewee relayed advice from lawyers who 'said to just sue...we still began to put in clauses around data leakage but the maximum fines for data breaches today are about US$50m vs. an internal cost of closer to US$1b.'

Both suppliers and miners have an interest in getting this right. A useful analogy for a mining company is a block of swiss cheese, the cheese being capital, brand and resources while the holes are all of the suppliers. Most operational activity in mining companies is completed by the supply chain, so the ultimate solution will lie in both groups being resilient individually and collectively in a system. Companies need to engage with their suppliers deliberately, ensuring security awareness, standards and capability is built into its supply chain.

Despite this, most of our data suggested that evaluations of supplier cybersecurity capability are sporadic or one-off, if at all. Selecting and evaluating vendors will become a key skill, potentially even moving in the direction of real-time evaluation as software capability improves. Scrutiny of suppliers will grow as mining companies become more mindful of the risk that suppliers pose to their overall cybersecurity exposure. Emerging digital business models such as servitisation will also shift the security onus towards suppliers. Anecdotally, this trend is still a fledgling concept for smaller service companies – there are few examples of non-cyber companies marketing cyber resilience as a core aspect of their value proposition. In time, we expect this to shift dramatically with 100% (every single person) we surveyed believed that a strong cybersecurity reputation will become critical or important for equipment and service companies over the next five years.

> "You and everyone you depend upon qualify as members of a virtual enterprise and cybersecurity must be seen as a blanket over all of you."

Is DIY enough?

Traditionally mining companies have relied on internal IT departments and more recently, specialist service providers as a source of cybersecurity capability. As the cyber threat grows, companies are increasingly looking to embed cyber-capability into their operations.

FIGURE 20

WE ASKED: WHAT IS YOUR PRIMARY SOURCE OF CYBERSECURITY CAPABILITY?

By % of respondents given one option

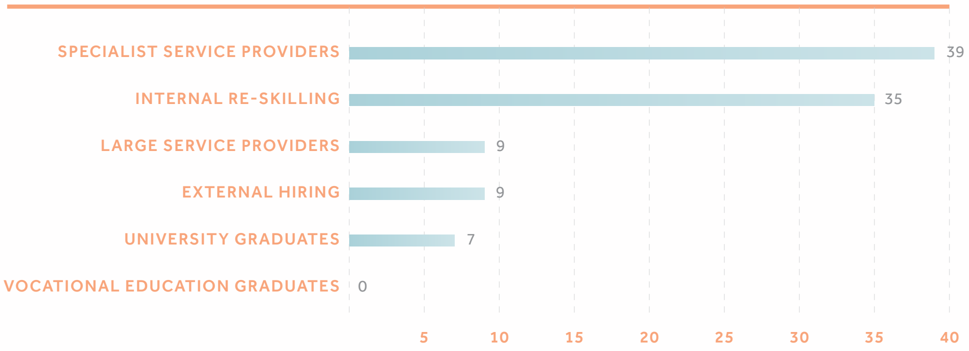
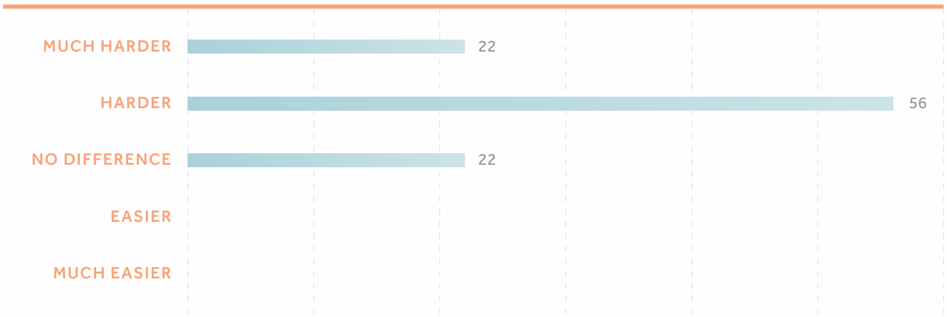


FIGURE 21

WE ASKED: HOW WOULD YOU DESCRIBE THE EASE OF ATTRACTING AND RETAINING SKILLED CYBERSECURITY PEOPLE, RELATIVE TO OTHER ROLES?

By % of respondents given one option



56% of survey respondents identified that attracting and retaining cyber skilled people into the mining industry was harder relative to other roles. In light of this companies have begun to invest in training, education and re-skilling of their existing workforce. The benefits of this are two-fold: the workforce retains its core mining knowledge, and its cyber-capabilities are improved.

A Catastrophic Catalyst

> "There are two types of mining companies: the ones that can foresee risk and act, and those that need to be pushed."

Deepwater Horizon. Samarco. Grenfell Tower. Fukushima.

Four well-known contemporary catastrophic events that have shaped their respective industries. Traditionally, the resources sector has required the occurrence of a significant catastrophic event before long overdue corporate and regulatory action is taken. This trend is expected to extend to cybersecurity in the mining industry, with 98% of survey respondents identifying that such an event would be required to drive a sector-wide response.

The threat to industrial systems should not be underestimated. We have already seen the rapid deployment of new and more destructive cyber-attacks across the industrial sector:

- Nuclear centrifuges in Iran damaged by malicious commands sent by Stuxnet destructive malware in 2010;
- Blast furnace in German steel mill damaged by malware which destroyed control system in 2014; and
- Interruptions to the Kiev power grid by the BlackEnergy malware attack in 2015.

A cybersecurity incident in the mining industry could take a variety of forms. A majority of respondents have identified that a physical incident would be more likely to galvanise a sector-wide response than a data breach. First movers in protecting industrial operating systems and suppliers who engage with this challenge will realise significant safety benefits.

FIGURE 22

WE ASKED: WHAT LEVERS DO YOU BELIEVE WILL DRIVE A SECTOR-WIDE RESPONSE TO CYBERSECURITY IN THE MINING INDUSTRY?

By % of respondents given two options

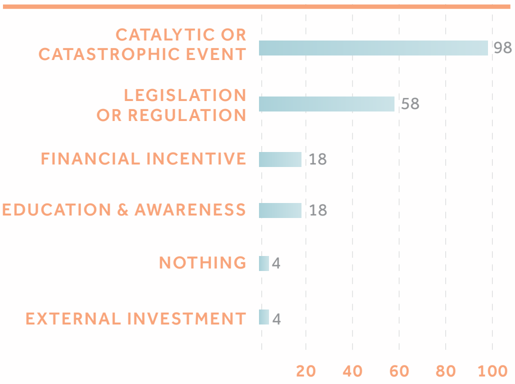
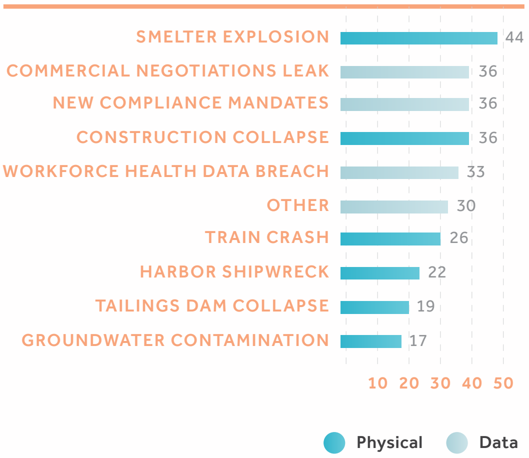


FIGURE 23

WE ASKED: WHAT CATALYTIC EVENT, CAUSED BY A CYBER-ATTACK, IS MOST LIKELY TO GALVANISE SECTOR-WIDE RESPONSE TO CYBERSECURITY?

By % of respondents given three options



CONCLUSION

Don’t Forget this is a Global Game

Over half of the people in the United States have already had their personal information exposed through cybersecurity attacks. Computers are inexorably getting faster, as is the speed of communications. Global financial transactions are growing exponentially in number and value. At the same time, governments of all persuasions are dedicating enormous budgets and political will for investing in cyber-attack and defence capabilities. Private companies, particularly in the United States and China, are rapidly increasing their investments in venture funds focused on cybersecurity.

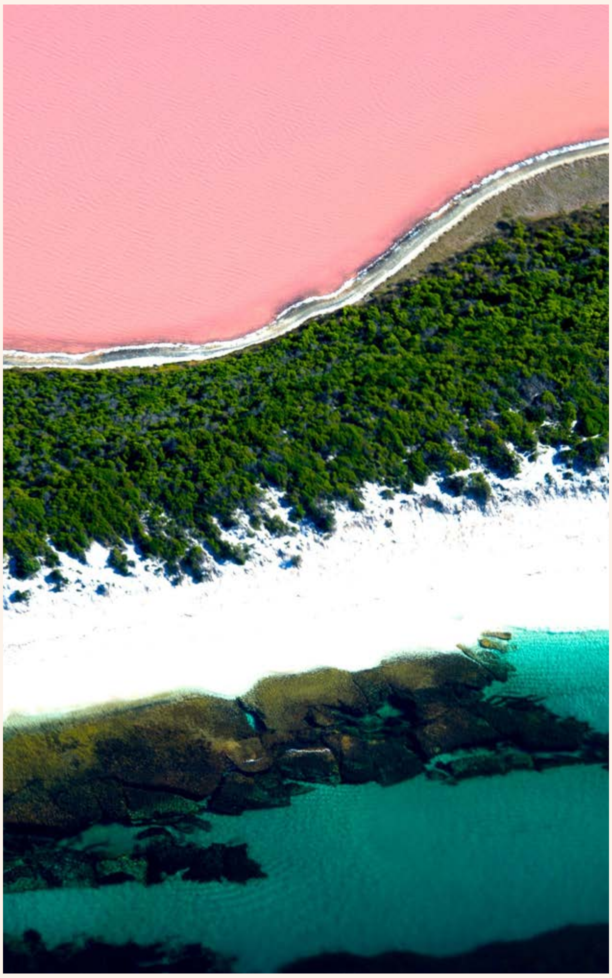
Much of what happens in this space over the coming years will be a case of impact more than influence for the mining industry.

It is clear that there are some areas in which the mining industry can and should take the lead, both because of competitiveness and specific risk. Doing so is both a necessity and an opportunity for the companies and countries that drive it. Mining has long dealt with low probability, high risk catastrophes – many of which have led directly to many negative external perceptions of it. In spite of this experience with strategic risk management, there is still a lot of scope to improve and modernise its approach. Cybersecurity offers a fantastic opportunity to be the catalyst for innovation in this space.

> “The question is whether we wait for it to happen and respond, or whether we are proactive.”

Digital transformation is the objective and distraction of contemporary executives and yet many are struggling to give it clear direction and effective implementation. Having spent the past year learning about cybersecurity in the mining industry, and how executives are managing it, the potential for cyber to become the driving force for achieving the fundamental step-change goals of digital transformation is both refreshing and tantalising. Legacy operations, technology and applications, however, will continue to be complex and complicating for some time.

When all is said and done, cybersecurity is all about the people. People who are motivated and incentivised to commit cyber-crime. People whose behaviours when using digital technology enable and arm much of the crime to happen. And the people tasked with defending their businesses from attack through the application of creativity and ever more sophisticated technologies. Perhaps becoming more aware of external behaviour and motivations will come benefit mining businesses more broadly with respect to collaboration with suppliers and engagement with social issues.



The State of Play team

Graeme Stanway
Paul Mahoney
Kevin Ong

State of Play

CYBERSECURITY

THE LINK BETWEEN STRATEGY,
INNOVATION AND SECURITY

STATE OF PLAY

VCI

Cognizant

METS IGNITED
Engage in our future

AustCyber
Australian Cyber Security Growth Network

STATEOFPLAY.ORG