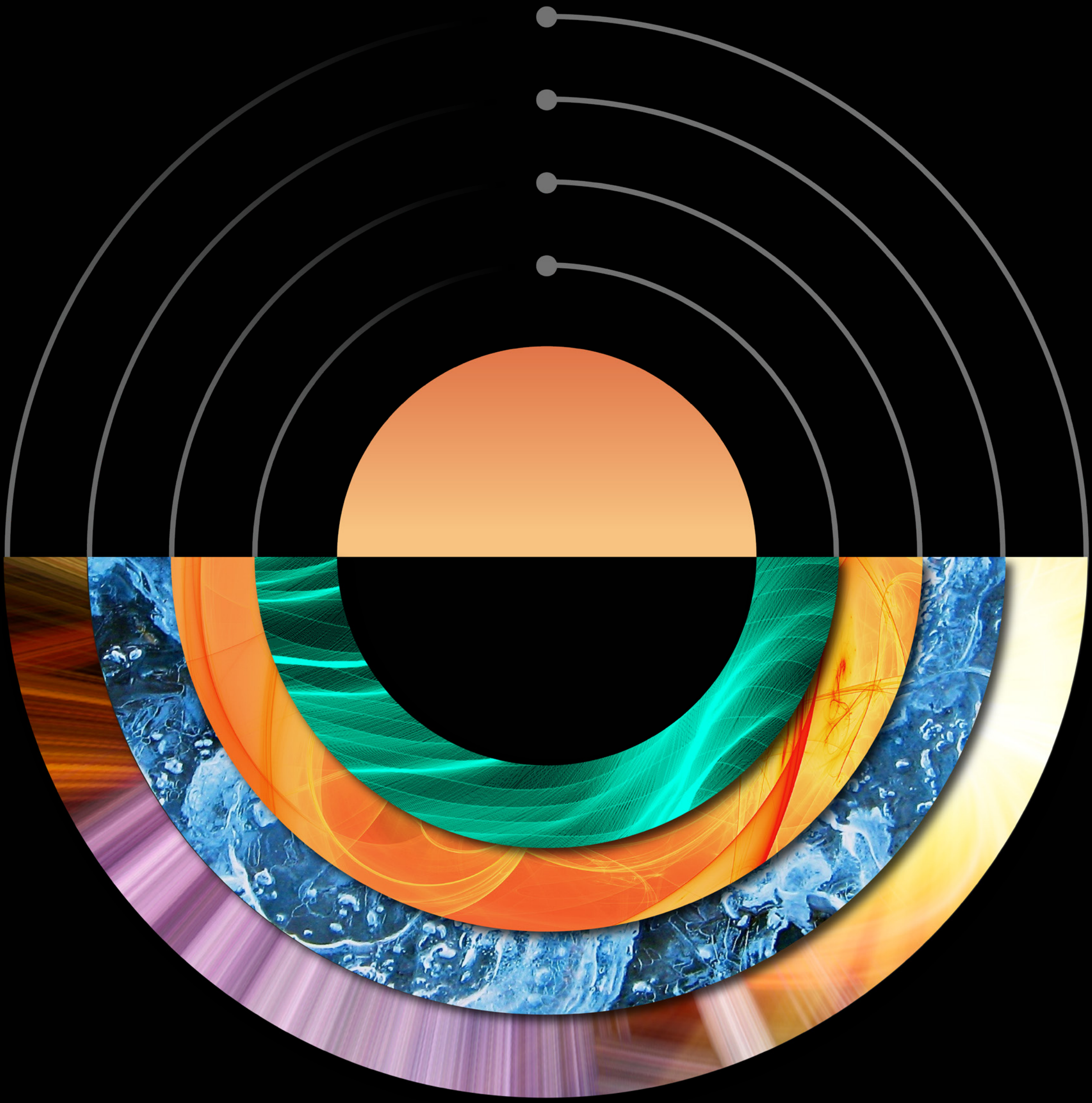
Deloitte.



Safety 4.0

A new horizon for
energy and resources safety

Contents

Introduction

It seems it was not that long ago that energy and resources executives and board directors focussed on two primary concerns—to ensure operational workers returned home safely to their families and to deliver the best possible shareholder returns. There were, and still remain, many other matters to deal with.

When it comes to leadership and accountability, the world has fundamentally shifted. When it came to accidents, incidents and poor behaviour, Australians were generally slow to judge and quick to forgive, but now we are quick to judge and slow to forgive. This is a significant change in the mindset of workers, customers, investors and society more broadly.

Today, the world we operate in is increasingly complex and this has shifted the dial in modern energy and resources safety—expanding into new terrain and adding further light and shade to traditional ones.

Worker safety is as critical as ever, but for energy and resources leaders, whether executives, directors or management, the challenge is no longer just keeping people safe physically but protecting their mental wellbeing—and this means creating a safe environment for everyone, one free from discrimination, intimidation, bullying, harassment and isolation, where everyone is respected and supported and diversity is embraced in all its forms.

Cyber safety is another terrain energy and resources leaders must increasingly tackle. Modern energy and resources operations are technologically advanced and vulnerable to cyber-attacks (including attacks on infrastructure) which are on the increase from adversaries around the globe. The buck stops with all leaders when it comes to responsibility for their organisation's cyber safety. As well as having the right teams, systems and processes in place to detect, defend and respond they must create a cyber safe culture where workers share this responsibility.

Modern energy and resources safety is multifaceted, but we've captured four key dimensions—what we call **Safety 4.0—the four layers of safety** that leaders must consider and work towards to create a safe, sustainable, inclusive, resilient and successful organisation. These will need the same level of ownership and commitment currently given to the more traditional view of safety.

By looking beyond the current landscape towards this new horizon of safety, energy and resources leaders can gain the perspective needed to succeed in an increasingly disruptive and challenging era. And those who embrace and integrate these layers of modern safety will be building secure foundations that safeguard their organisation and its people into the future.

The Safety 4.0 report will set you on the right course to achieving this goal, but the true key to success lies with leaders at the heart of every organisation. It's up to you all to set the right tone and role model what's acceptable and what's not. The reward will be a safer, more prosperous and sustainable future for everyone. The penalty will be loss of reputation and all that comes with it.

Four dimensions of Safety 4.0

Our **four layers** of safety link and build on each other to create foundations for a secure organisation.

Physical safety extends into all areas of the workplace and must combine with psychological safety to ensure mental health and wellbeing. For this to be successful cultural safety must be embedded to create a safe environment for all people, regardless of age, gender, sexual preference, race, religion or socio-economic status. Cyber safety underpins the entire organisation and a layer that is dependent on every worker sharing in the responsibility. These four layers work together and interlink to create a new horizon of safety for the energy and resources industry.

1.0 Physical safety

Continuing to put the safety of workers at the forefront of all operational interactions is paramount. This thinking needs to extend to the redesign of all of the physical environments workers are in, from core operational areas to accommodation and living facilities, to transportation and offices. Energy and resources leaders should take accountability for thoughtful design and operation to ensure individuals are safe from accidents, assaults, or any threats to their physical wellbeing.

2.0 Psychological safety

The second dimension is foundational to the energy and resources industry achieving the required level of innovation spoken about for so long. Leaders need to ensure the organisations they lead are genuinely places of psychological safety. This means providing a workplace where people can bring diversity of thought, innovation and new ideas and that these conversations are valued and explored, safe from intimidation, bullying, harassment or isolation.

3.0 Cultural safety

This third area of safety is a relatively new concept that explores and aspires executives, directors and management to lead and become an organisation where everyone can be proud of who they are regardless of culture, ethnicity, age, sexuality and gender. In an environment of cultural safety, energy and resources organisations respect their people and the communities they operate in, as well as valuing and protecting the culture of the lands on which they operate.

4.0 Cyber safety

Energy and resources leaders are responsible for cyber security. The SOCI Act requires any system of national significance (SONS) to have a risk management plan which mitigates personnel hazards, physical and natural hazards, cyber security hazards, and supply chain hazards. Energy and resources companies must take cyber safety seriously, or risk damage to their assets, reputation and future.

This report outlines the key considerations for each of these dimensions in more detail, provides key questions energy and resources leaders should ask and actions leaders should take and suggests information and opportunities to take proactive steps to be at the forefront of safety.

1.0 Physical safety

We've seen many changes to workplace health and safety over the past few decades, but despite stronger legislation, there are still significant workplace injuries in the energy and resources sector, with a huge cost to workers, their families and the community.

The most recent mining industry figures show that **10** people were killed in the Western Australian (WA) mining and exploration industry in a five-year period.[1]

There were also **402** serious lost-time injuries reported in WA mining in 2020–2021.[1] These included significant, often life-changing injuries with ongoing rehabilitation costs and wider social and psychological impacts on individuals. The most common physical workplace injuries in mining are muscular skeletal, which made up **73%** of all injuries documented in the final quarter of 2021.[1]

So, what's new in the realm of physical safety and health and how can we reduce these statistics further in the coming years?

For the first time in nearly **30 years**, we have new WHS Legislation in WA with the introduction of the WA Work Health and Safety Act 2020 and the WA Work Health and Safety Regulations (mining and General) 2022. There are key legislation changes that could impact the broader ER&I sector, including:

1. Key Terms and Definitions
2. Industrial Manslaughter
3. Enforceable Undertakings
4. Health includes psychological health

01. Key Terms and Definitions

A significant change to the WA WHS legislation is the addition of the term 'Person Conducting a Business or Undertaking' (PCBU). The PCBU is the primary duty of care holder in a workplace and includes a much broader, more inclusive number of workplace relationships than the former concept of 'Employer'. Moreover, on a mining worksite multiple people across different businesses meet the definition of PCBU adding complexity and accountability for all those who hold the primary (chief) duty of care for workers at any one time.[2]

The term 'Worker' has also been adopted in place of 'employee' and includes any person, including an employee, contractor, sub-contractor, self-employed person, outworker, apprentice or trainee, work experience student, labour hire employee and volunteers, basically anyone who carries out work. This comprehensive definition ensures most people on an operational site are owed a duty of care by you as energy and resources leaders and in turn hold a duty to others.[2] The revision of this term ensures that no sub-group is excluded, and the duty of care owed to these groups is now clear.

Finally, the term 'Officer' has been introduced to the legislation and includes people who make or participate in making decisions which affect the whole, or a substantial part, of the organisation's activities. The WA Work Health and Safety Act 2020, places a duty on officers to exercise due diligence to ensure the PCBU complies with its health and safety duties. Put simply if you are in a leadership position you are an officer for the purpose of the Act, and it outlines a comprehensive list of what should be included in the due diligence process that energy and resources leaders are responsible for.[2]

02. Industrial Manslaughter

The new WA WHS Act 2020 includes a provision in which leaders can be charged with the offence of industrial manslaughter. The WA government included this provision based on concerns raised by families of workers killed in WA workplaces, as well as two national reviews into workplace fatalities.[4,5]

Industrial manslaughter is a criminal offence under the WA WHS Act 2020 occurring when someone in a decision-making position knowingly engages in conduct likely to cause death or serious harm and includes a failure to comply with their health and safety duties. It carries significant fines and a penalty of up to 20 years imprisonment if negligence is proven.[3]

It's a significant addition to the legislation and is no doubt designed to have a deterrent effect on energy and resources leaders regardless of the position within the organisation. It enforces the requirement to carry out due diligence on workplace hazards. It also aligns industry practice with community expectations around acts of negligence.

03. Enforceable Undertakings

As an alternative to prosecution, the new WA Work Health and Safety Act introduces the concept of 'Work Health and Safety Undertakings'. These undertakings are given to the regulator by a person in an organisation to address a contravention of the WHS legislation. Once accepted in writing by the regulator it becomes enforceable and the organisation must comply. [2] This new approach is a positive step forward and opens the way for energy and resources leaders to work collaboratively with the regulator to address WHS outcomes.

04. Health includes psychological health

Another significant change to the new WA WHS legislation is the expansion of the term 'health' to include not just physical health but also psychological or mental health.

Psychological hazards in the workplace could include issues such as the nature and design of the work, workload, work hours, work pressures, isolated work, workplace design, workplace facilities, acts of violence, bullying, aggression and harassment.

As with any workplace hazard, energy and resources leaders must ensure they conduct a thorough WHS risk assessment of the psychological hazards impacting all areas of their workplace. These risk assessments should include a full review of all workplace activities and interactions and consider how psychological hazards impact physical hazards, as well as how injury can include psychological aspects which further exacerbate an injury.

2.0. Psychological safety

Recognising the importance of psychological safety in providing a holistically safe workplace is key to the shift in mindsets needed in many workplaces.

An inclusive approach

The recent media spotlight on the energy and resources sector, driven in part by various high-profile cases, industry reviews and investigations, highlights the need for a more inclusive approach to safety.

So, what does psychological safety mean and why is it so important for workplaces to consider?

Harvard Business School Professor, Amy Edmondson defined psychological safety as **'an absence of interpersonal fear'**.[6]

When people feel engaged, free to speak up on issues, input ideas, raise areas of concern or admit mistakes and to challenge ways of working, they feel included. Workers sense a feeling of trust in the organisation that they'll be able to speak up and make a valued contribution without fear of retribution, humiliation, or punishment.

There are many benefits to organisations when workers are engaged and feel safe, including increased productivity, reduced attrition and a positive brand in the market.

Contemporary inquiries recognise the importance of psychological safety. *Set the standard: Report on the Independent Review into Commonwealth Parliamentary Workplaces* revealed

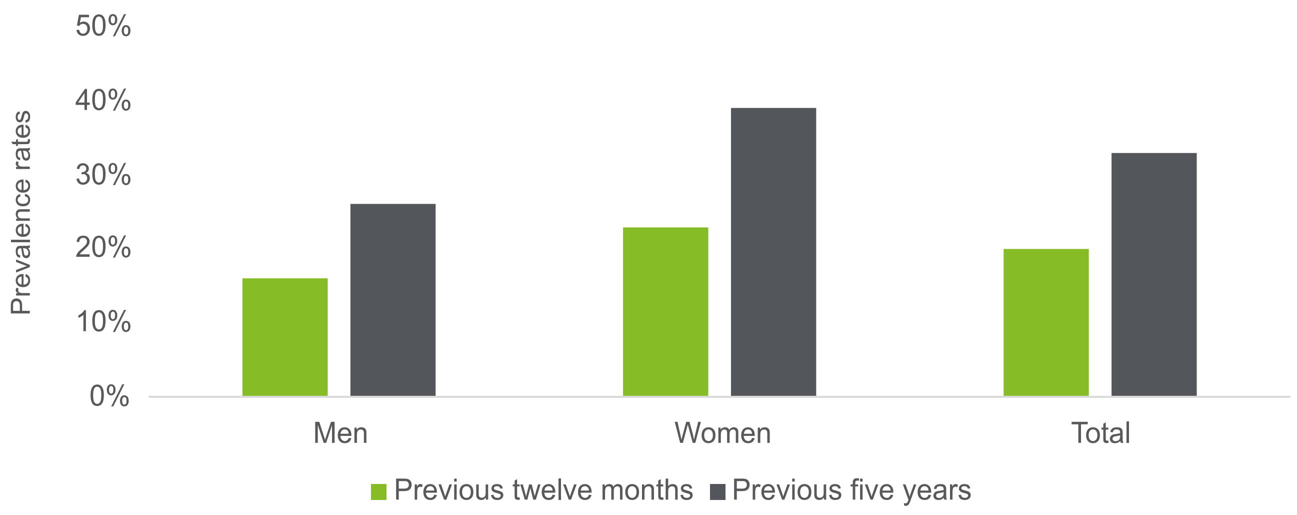
> **"greater levels of psychological safety does not only encourage workers to report a broad range of workplace harms, thus improving safety, but also contribute more generally to inclusion and collaboration".**[7]

A Western Australia Parliamentary report into sexual harassment against women in the FIFO mining industry galvanised the need for broader ER&I leaders to reflect on what they're doing to provide a psychologically safe environment for women.

This report also provided evidence that there is significant underreporting of inappropriate workplace behaviours, demonstrating how victims and bystanders do not feel safe in their environments to speak up.[8]

Analysis by Deloitte Access Economics (DAE) measured the total financial cost of workplace sexual harassment to the Australian economy in 2018 was **$3.8 billion**, the largest component of which is lost productivity **($2.6 billion)**. Mining contributed **$110.5 million** to that lost productivity and an additional economic cost of **$20.7m**.[9]

Prevalence of workplace sexual harassment by gender



Source: The economic costs of sexual harassment in the workplace; final report. Deloitte Access Economics, March 2019

Next steps

It's incumbent on energy and resources leaders to rewrite the industry narrative and create workplaces that genuinely embrace psychological safety, strengthen worker trust and shift the dial from reactionary to preventative measures. Societal expectations for transparency and accountability have changed, regulatory and compliance obligations are tighter and the labour market tougher. Energy and resources leaders will need to pay particular attention to proactively providing an inclusive and psychologically safe working environment if they're going to meet their legislative and moral obligations, retain workers and attract the diversity of talent required for their future workforce. Moreover, leaders are expected to act quickly to address incidents and take corrective actions in the best interest of the injured worker.

Action

- **Understand the problem:** Listen deeply to your people to understand what factors may be inhibiting psychological safety for workers.
- **Perform a risk assessment and take a risk management approach:** Identifying hazards and associated risks—practical early action and controls—can prevent workplace incidents. Psychological hazards must be managed the same way as all other WHS hazards.
- **Set the standard:** This means identifying the broad, underlying cultural factors contributing to perceptions or feelings of being psychologically unsafe.
- **Revise** your policies, systems, processes, structures, worksites, symbols, norms and accepted daily behaviours to ensure people are safe at work.
- **Drive programs that educate and shift existing mindsets:** This must be modelled from the top and includes measuring the impact of actions taken to understand how they've changed mindsets and consequential behaviours.
- **Monitor and report** incidents and the actions taken to investigate and resolve.

3.0 Cultural safety

A culturally safe workplace creates an environment where people are respected, supported, heard and celebrated whatever their cultural identity, a place where their needs are met and where they fear no challenge, denial or assault because of who they are. To be culturally safe, people need to know that their whole health and wellbeing is understood and supported.

When you are at work, you shouldn't have to change who you are to feel safe. While a diverse workplace does not guarantee cultural safety, lack of diversity in leadership and workforce will contribute to lower cultural safety.

Many workplaces aren't adequately addressing cultural safety and at times when poor cultural interactions occur they are explained away as 'excusable' ignorance. Reporting of poor cultural safety will provide leaders with an early-warning system for serious HR incidents, such as bullying, assaults and psycho-social injuries. Ignorance is not an excuse. Workers, communities and stakeholders increasingly hold organisations to high standards and—in an age of greater transparency, reporting and stakeholder activism—there's nowhere to hide.

Smarter, more effective organisations

Diverse workforces are more capable and effective and enable greater cultural safety.

There are many benefits for organisations who embrace cultural safety. When workers are culturally safe, they speak freely—which increases innovation and diversity of thought. They explain different perspectives—getting your company closer to client views. They will challenge practices that make them feel uncomfortable—which supports good conduct and culture. They can be seen other than through their 'differences' allowing them to bring their networks and knowledge to work. They will be more resilient due to increased wellbeing and therefore adapt more easily to change. They will feel safe to challenge the status quo by articulating why something isn't working—preventing echo-chambers of agreement.

A culturally safe workplace helps people call out safety issues leading to decreased injury. Cultural safety attracts, engages and retains talent when people feel valued while bringing their whole selves to work.

Is your organisation culturally safe?

The first step is to understand your organisation's diversity and its cultural safety baseline. This can be done by considering your people metrics, using qualitative data such as conversation themes and by piecing together what is happening through people movements across teams.

Once you have a baseline you can start putting strategies in place to move the organisation towards one that is culturally safe for all people. The four key strategies needed are: [10]

1. Listen, learn, change the script
2. Decode power and privilege
3. Look back to move forward
4. Learn from and partner with Indigenous Australians

01. Listen, learn, change the script

Do your organisation's stories reflect your people? Historically, the stories told and voices heard across organisations and industries have had a narrow perspective, overlooking the cultural diversity of their workforce or the communities they serve. But many people will have contributed to your organisation and it's time to discover, listen, learn and lift minority voices so they can tell their stories, their way.

Safety requires honesty and integrity.

Australia's former Chief of Army, Lieutenant General David Morrison shared his success spearheading a gender equality, diversity and inclusion army initiative,

> **"By reviewing our culture, we found that our stories were exclusive, not inclusive. The stories you tell miners of the future cannot be represented by one gender or one ethnic demographic."**[11]

Action

Recognise and foster an understanding of minority groups to realise how they help build and improve your organisation. Provide opportunities for minority groups within your workforce to be part of telling the organisations' story—internally and externally. Ensure that contributions from minority community groups, organisations and businesses are recognised and honoured through organisation celebrations and communications.

02. Decode power and privilege

Beyond overt behaviours that are legislated against, it's also important to consider covert processes, policies and systems so you can understand, recognise and recalibrate the power imbalances that contribute to poor cultural safety in your organisation. This includes:

- Putting recruitment processes under the microscope to ensure end-to-end inclusivity.
- A focus on co-creation, rather than consultation, to address power differentials at the start of new activities.
- Enabling reverse mentoring across hierarchies and between people of diverse cultural groups.
- Measuring representation and making this transparent to workers, as well as asking for their support to make changes.
- Recognise and reward leaders who achieve greater diversity and cultural safety.

Action

- **Identify the demographics** of your last 100 hires. Does your organisation consist of a diverse workforce or is there opportunity to increase the diversity?
- Create a **cross-cultural mentoring** or coaching program.
- Have a **demographic dashboard** on display to celebrate the value of diverse thought and problem solving that makes up your workforce.

03. Look back to move forward

Reflecting on and learning from past experiences, known as collective reflective practise, enables discussions, critiques and viewpoints that increase cultural safety for everyone across the organisation. It considers what hasn't been said and gives insight into the power dynamics excluding certain voices.

Collective reflective practice develops continuous improvement, enables change through feedback, develops organisational alignment through self-awareness and should be a requirement for all leadership roles.

One way of doing this is to consider whose voice isn't present in the room. It can also be helpful to think about the meeting after the meeting, which is often a core group of aligned decision-makers who then decide what will happen. When small groups of unknown people make quick decisions in the name of effectiveness it can signal elitism and a perception of poor transparency throughout the workplace.

A framework for collective reflective practise can support the change required for cultural safety.

Action

- **Regularly review** your understanding of cultural safety.
- Get **honest and frank feedback** on performance against cultural safety metrics, which are included in your capability frameworks.
- **Assess your leadership** against cultural safety metrics.

04. Learn from and partner with Indigenous Australians

Australia is also home to the longest continuous living culture on earth, which has survived because of its deeply embedded knowledge, culture, and protection of Country. There is an opportunity to move from historically transactional, rights-based, contractual partnerships with Indigenous peoples, to values-based relational partnerships. Partnerships bring the opportunity of reorienting our trajectory away from irreversible damage to our environment, towards regeneration and sustainability.

Action

- Create **flexible working arrangements** and opportunities to advocate for cultural considerations applicable to roles.
- Create **robust metrics and reporting** by collecting Indigenous employment data to ensure that there is an equitable representation of Indigenous workers across the organisation, which in turn ensures a richer makeup of workforce, and/or to prioritise identified (Indigenous specific) recruitment practices in line with the organisation's commitment to Closing the Gap on Indigenous disadvantage.
- **Prioritise equal access** to learning, development and training opportunities for Indigenous workers and Indigenous representation at senior levels to achieve parity of Australian demographic and retain an Indigenous workforce.
- Understand **wellness priority** of your teams (this action is applicable for all team members) by co-creating a list of priorities and the benefits it will bring to the workforce.

4.0 Cyber safety

Innovation and the increasing use of technology in energy and resources, like automation, drones, artificial intelligence and advanced diagnostics, are transforming energy and resources, reducing costs and accelerating exploration. However, these technologies are vulnerable to hacking and require planning and threat analysis before they're used.

Workers, customers and suppliers place trust in us when providing their confidential information and the buck stops with energy and resources leaders to ensure their organisation is cyber safe.

With cyber-attacks in Australia—including attacks on our infrastructure—increasing from adversaries around the globe and federal laws requiring organisations to act, the task is harder than ever. Cyber safety must be a fundamental part of energy and resources organisations' safety planning.

Common energy and resources cyber myths that give a false sense of security

Myth

Technologies can only be hacked if they're connected to the Internet.

A common misconception is that technology is safe from malicious actions if it is not connected to the Internet.

Truth

Technologies can be compromised at any stage of their lifecycle and don't have to be Internet connected to be vulnerable. Some of the most successful hacking incidents have been on technologies not Internet connected.

Myth

You'll know if you've been hacked.

Truth

Most hacking doesn't seek to immediately cause disruption and many are intended to gather information. It commonly takes more than a year for a breach to be detected.

Myth

We're too small to be a target.

Truth

You are a probable hacking target if you are Listed on ASX; export or import anything; have any international shareholders or presence.

Myth

Our safety systems won't be impacted.

Truth

Many energy and resources companies have found that safety critical systems assumed to be separated from the Internet have been potentially compromised by accidental, temporary or unauthorised Internet connections. Even short periods of connection to the Internet can compromise these systems.

Some seemingly small events that have compromised critical systems include charging a phone on a safety system or plugging into critical plant in order to watch TV in the lunchroom.

It's not always about the cost.
Often the conversation about cyber breaches and technologies focuses on how much money was stolen, how much revenue was impacted, or how much the defensive technologies, processes and consultant costs. These are all important but may not be the most important aspects of a breach and the recovery—**it's not always about the monetary cost.**

Workers leave after a cyber breach

Worker retention loss commonly increases to **50%** after a high-profile cyber breach. For many companies, the move from **20% to 30%** annual staff turnover or higher can be the difference in meeting supply and customer service commitments or not.

Workers leave after a cyber breach for three main reasons:

- The perceived breach of trust that they had placed in their employer with their personal, family, health and banking information.
- The embarrassment they feel, both at work and in their community life, about the resultant media and social discussion about the breach.
- Failures in communication from their employer about the breach with their own workers, the customers and in the media.

A cyber breach does not mean failure.

When it comes to cyber security planning, it's a matter of when, not if. While many cyber breaches are preventable and caused by failures in planning, it's also true that for many cyber breaches the organisation breached has shown due diligence.

Defence in depth

We do everything possible to prevent breaches but also accept that a completely secure environment would be difficult to work in and would probably cost too much to achieve. What we can do is layer our defences so there's gradual trade-off between practical requirements of work, requirements for an effective cyber-defence, cost and the protection of information and operations. These layered defences place the greatest protection around the most valuable information while still being cost-effective and allowing the core business to continue.

The systems are working

Cyber professionals say the world is divided into two halves, those who know they've been hacked and those who don't. Advanced cyber-attacks commonly have a detection time of more than a year, frequently longer, so having the tools, processes and talent to detect a cyber breach can be proof your organisation has succeeded in cyber planning.

However, in the case of a breach, energy and resources leaders need to ensure there is a recovery plan and this should include a communications and therapy plan, with different communications required for workers, customers, shareholders, stakeholders, regulators and the media.

The recovery plan

The cyber response plan needs to include how the breach will be communicated. Different communications are required for workers, customers, shareholders or stakeholders, regulators and media.

Staff communication plans needs to include both the offer of therapy and pre-planning that therapy will be available. Privacy breaches in particular are known to cause mental health issues for workers whose own data may have been breached or who find themselves in the difficult task of explaining the breach to customers.

The foundation of the strategy is to plan to prevent as many cyber incidents as possible but to have a communications plan prepared if a cyber incident does happen.

An example of the impact of effective communications planning is two companies who suffered breaches of similar magnitude and severity within a few weeks of each other.

Planning pays

The first company had an effective recovery and communications plan.

They put plans in place to safeguard against a potential future cyber incident. Their planning meant workers had been nominated and trained to speak with the media following an event. Briefing notes had been prepared to guide workers on conversations with customers. Customers were informed—as were workers and shareholders—prior to the media.

The company worked actively with the police and other regulators to both investigate the incident but also minimise the investigation's operational impact.

The result? Minimal customer, staff retention and media impact and they quickly resumed normal operations.

No plan...everyone pays

The second company didn't have a communications plan.

The company's first briefing to the media was inaccurate, incomplete and required several revisions. Workers had not been trained in how to speak to the media about a cyber incident—making them look unprepared and inefficient. Customers learnt about the incident from the media, as did workers and shareholders. Workers weren't trained or given guidance when speaking with customers and because there wasn't a plan on how to work with police and regulators, the investigation held up the resumption of normal operations.

The result? The company lost a third of its customers, its CEO, plus staff turnover increased by 60% and it was in the media for months, causing serious, ongoing reputational damage.

Security of Critical Infrastructure Act

This federal legislation first became law in Australia in 2018 and has been significantly strengthened in 2021 and 2022. This new legislation now acts in parallel with the Australian Privacy Act to provide a basis for trust for cyber security in the companies to which these acts now apply. The SOCI Act requires any system of national significance (SONS) must have a risk management plan—the four main elements of the plan are:

- Personnel hazards
- Physical and natural hazards
- Cybersecurity hazards
- Supply chain hazards

For energy and resources leaders the requirements for both cyber trust and SOCI are common sense. In most cases they'll require limited or minimal investment in new technology and staff. In both cases the emphasis will be on risk management and communications planning. Once established the key consideration must ensure these plans are updated and remain current as people and the organisation change.

Action

- **Review your processes** for onboarding and removing contractors. Many energy and resources companies are surprised to learn that their contractor agencies have not done basic background checks. In some cases they have rehired contractors who were terminated for cause, less than a month earlier.
- Conduct a **cyber threat assessment** before adopting new technologies, particularly those which use automation such as robots, drones, remote management, advanced diagnostics or artificial intelligence.
- Any computer dependent system can be hacked, it does not need to be connected to the Internet. **Controls need to be in place** to detect unauthorised connections or activity for critical systems such as operational plant and safety systems.

Conclusion

In this increasingly transparent world with society expectations of greater responsibility and accountability, energy and resources leaders need to up the ante on all aspects of safety.

An energy and resources organisation that can truly demonstrate leadership on each layer of Safety 4.0 will not only reduce the likelihood of injury to workers and loss of reputation, it will become more attractive to workers, shareholders, community groups and government partners.

There are real opportunities for organisations that lead on safety:

Physical safety attracts workers from all walks of life to enjoy the working environments provided by an energy and resources organisation.

Psychological safety attracts innovation and diversity of thinking, encouraging workers and partner organisations to challenge the status quo and explore opportunities for new ways of working.

Cultural safety encourages communities to welcome energy and resources organisations onto their land and into their regions and strong working relationships across cultures can provide opportunities for collaboration and streamlined approval processes.

Cyber safety enables workers, customers, suppliers and shareholders to place their trust in an organisation with their confidential information and the responsibility for taking care of their careers, businesses and investments.

> Each element of Safety 4.0 is an opportunity for our industry. Energy and resources leaders who can seamlessly integrate and have genuine engagement, action and advocacy for all aspects of safety will lead their organisation towards a more sustainable, secure, resilient and prosperous future.

References

1. Safety Performance in the Western Australian Mining Industry: Accident and Injury Statistics 2020-21. Department of Mines, Industry Regulation and Safety, 2021
2. Overview of Western Australia's Work Health and Safety Act 2020. Department of Mines, Industry Regulation and Safety, 2021
3. Work Health and Safety Act 2020. State of Western Australia. Department of Mines, Industry Regulation and Safety, 2021
4. Review of the Model WHS laws: Final Report. M Boland. Safe Work Australia, 2018
5. Federal Senate Inquiry: They never came home—the framework surrounding the prevention, investigation, and prosecution of the industrial deaths in Australia. Commonwealth of Australia, 2018
6. CHRO Quarterly. Gartner Human Resources Practice. Third Quarter 2019
7. Set the Standard: Report on the Independent Review into Commonwealth Parliamentary Workplaces. Australian Human Rights Commission, November 2021
8. Report 2 'ENOUGH IS ENOUGH' Sexual Harassment against women in the FIFO mining industry. Community Development and Justice Standing Committee of the Legislative Assembly of Western Australia. June 2022
9. The economic costs of sexual harassment in the workplace; final report. Deloitte Access Economics, March 2019
10. Deloitte's framework is aligned to principles found in Translating Cultural Safety to the UK—Scientific Figure on ResearchGate.
    Available from: https://www.researchgate.net/figure/The-Cultural-Safety-Tree-in-table-format-Translating-Cultural-Safetyto- the-UK_tbl1_353345768 (accessed 3 Jul, 2022)
11. Mining: what story are we telling? Let's change the conversation. Deloitte, 2019
    Available from: https://www2.deloitte.com/au/en/pages/energy-and-resources/articles/mining-change-conversation.html

Acknowledgements

Alongside the team of specialists that worked on this report (listed overleaf), we also thank Steven Walsh, Kris Rodgers, Sonia Lindsay, Helen Carbone and Jimmy Watson-Galbraith at Deloitte, for providing their time, support and valuable contributions in creating this report.

Contact us

It's time to head towards a new horizon of energy and resources safety and we're here to help. Reach out to our team of specialists, who work every day to support energy and resources organisations to be truly leading in Australia and across the world.

Nicki Ivory
Mining & Metals Leader—Australia
Ph: +61 89365 8050
nivory@deloitte.com.au

Bernadette Cullinane
Energy & Chemicals Leader—Australia
Ph: +61 89365 7137
bernadettecullinane@deloitte.com.au

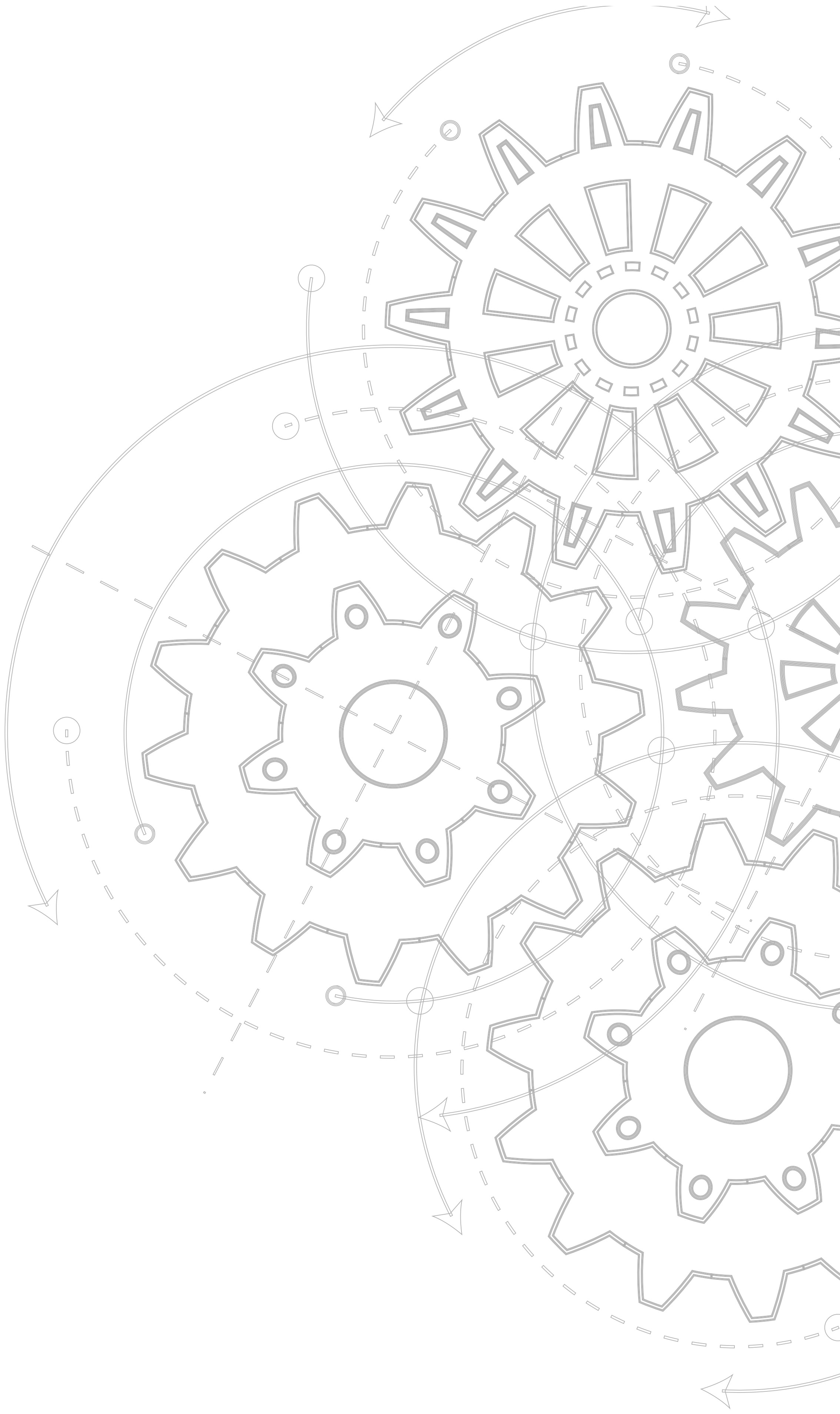
Kellie Properjohn
Respect at Work
Ph: +61 89365 8050
kproperjohn@deloitte.com.au

Luke Forsyth
Cyber Security
Ph: +61 89365 8010
lforsyth@deloitte.com.au

Kristy Delaney
Workforce Design & Transformation
Ph: +61 89365 7163
kdelaney@deloitte.com.au

Samantha Jones
Work Health & Safety
Ph: +61 28260 4137
samanthajones@deloitte.com.au

Rebecca Halliday
Indigenous Services Group
Ph: +61 28260 6076
rhalliday@deloitte.com.au



Deloitte.

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively the "Deloitte Network") is, by means of this publication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities. DTTL (also referred to as "Deloitte Global") and each of its member firms and their affiliated entities are legally separate and independent entities. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

About Deloitte
Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our network of member firms in more than 150 countries and territories serves four out of five Fortune Global 500®companies. Learn how Deloitte's approximately 286,000 people make an impact that matters at www.deloitte.com.

About Deloitte Asia Pacific
Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities provide services in Australia, Brunei Darussalam, Cambodia, East Timor, Federated States of Micronesia, Guam, Indonesia, Japan, Laos, Malaysia, Mongolia, Myanmar, New Zealand, Palau, Papua New Guinea, Singapore, Thailand, The Marshall Islands, The Northern Mariana Islands, The People's Republic of China (incl. Hong Kong SAR and Macau SAR), The Philippines and Vietnam, in each of which operations are conducted by separate and independent legal entities.

About Deloitte Australia
In Australia, the Deloitte Network member is the Australian partnership of Deloitte Touche Tohmatsu. As one of Australia's leading professional services firms. Deloitte Touche Tohmatsu and its affiliates provide audit, tax, consulting, and financial advisory services through approximately 8,000 people across the country. Focused on the creation of value and growth, and known as an employer of choice for innovative human resources programs, we are dedicated to helping our clients and our people excel. For more information, please visit our web site at www.deloitte.com.au

Liability limited by a scheme approved under Professional Standards Legislation.

Member of Deloitte Asia Pacific Limited and the Deloitte Network.

© 2022 Deloitte Touche Tohmatsu.

Designed by CoRe Creative Services. RITM1136964