hsi donesafe | solv

Selling safety to executive teams:

WHAT YOU CAN LEARN FROM CYBERSECURITY'S SUCCESS.

REFRAMING SAFETY

It's no secret that safety is still under-sold. Cybersecurity gets attention. Safety, less so.

Despite both carrying significant operational and reputational risk, executive teams typically dedicate more budget and strategic time to cyber threats than to workplace safety.

This article explores how safety professionals can take a page from the cyber playbook. It's a guide to reframing safety as a business risk - not a safety function - so you can unlock greater buy-in, faster decisions, and real investment.

> "If safety isn't part of the broader risk conversation at the executive level, then it will always be seen as a compliance function rather than an enabler."

Darren Evans
Health and Safety Risk Specialist

1

STOP SELLING SAFETY AS A MORAL OBLIGATION. SELL IT AS A RISK THAT HAS MAJOR CONSEQUENCES.

Executives don't make decisions solely based on what's "morally right". They need to do what's right for the organisation. The result? They act on risk, cost, and impact.

And cybersecurity leaders understood this early.

Take a moment and think about your IT and cybersecurity teams in your business.

They talk in terms of threats, breaches, and exposure. They focus on the cost of inaction and the probability of disruption. The fear of a catastrophic breach burns brightly, even though you can't recall a major event.

Sound familiar to safety?

The great news is, that safety teams can do the same. Instead of relying on incident rates or 'how many training hours we ran', reframe the conversation:

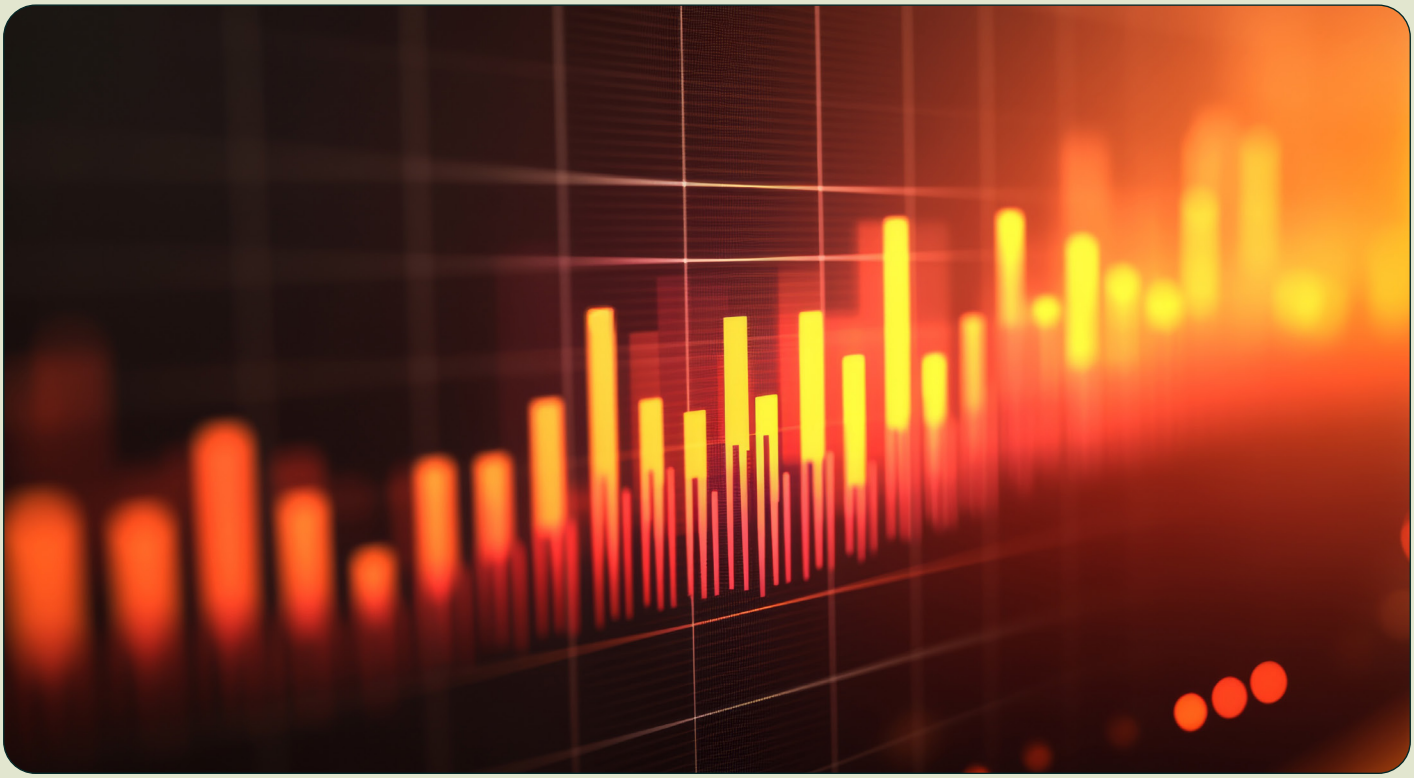
- → What would happen if a contractor is injured?
- → What does an unmitigated risk mean for downtime, fines or insurance costs?
- → What's the reputational cost if your name's in the paper, the news, or worse, an incident goes viral?

And just like cybersecurity, the risks are similar. The chance of injury is ever-present despite all the policies, processes, and training. Importantly, the right system will serve to mitigate the risk.

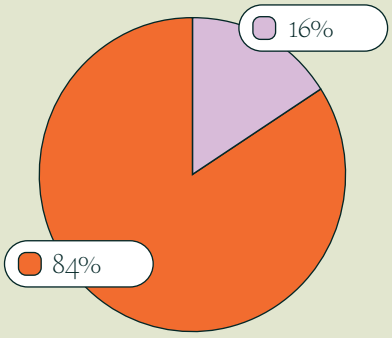
So, make safety a risk story - not a reporting exercise.

2

DON'T LEAD WITH LAGGING INDICATORS.



DISJOINTED SYSTEMS INCREASE YOUR RISK



- Don't use an integrated safety platform
- Uses an integrated safety platform

You can't sell a strategy on past results. That's where many safety conversations go wrong.

Metrics like LTIs or TRIFR might be essential for benchmarking, but they don't move the board.

Cyber teams don't lead with how many phishing emails they blocked last month - they talk about avoided costs, future threats, and systemic vulnerabilities.

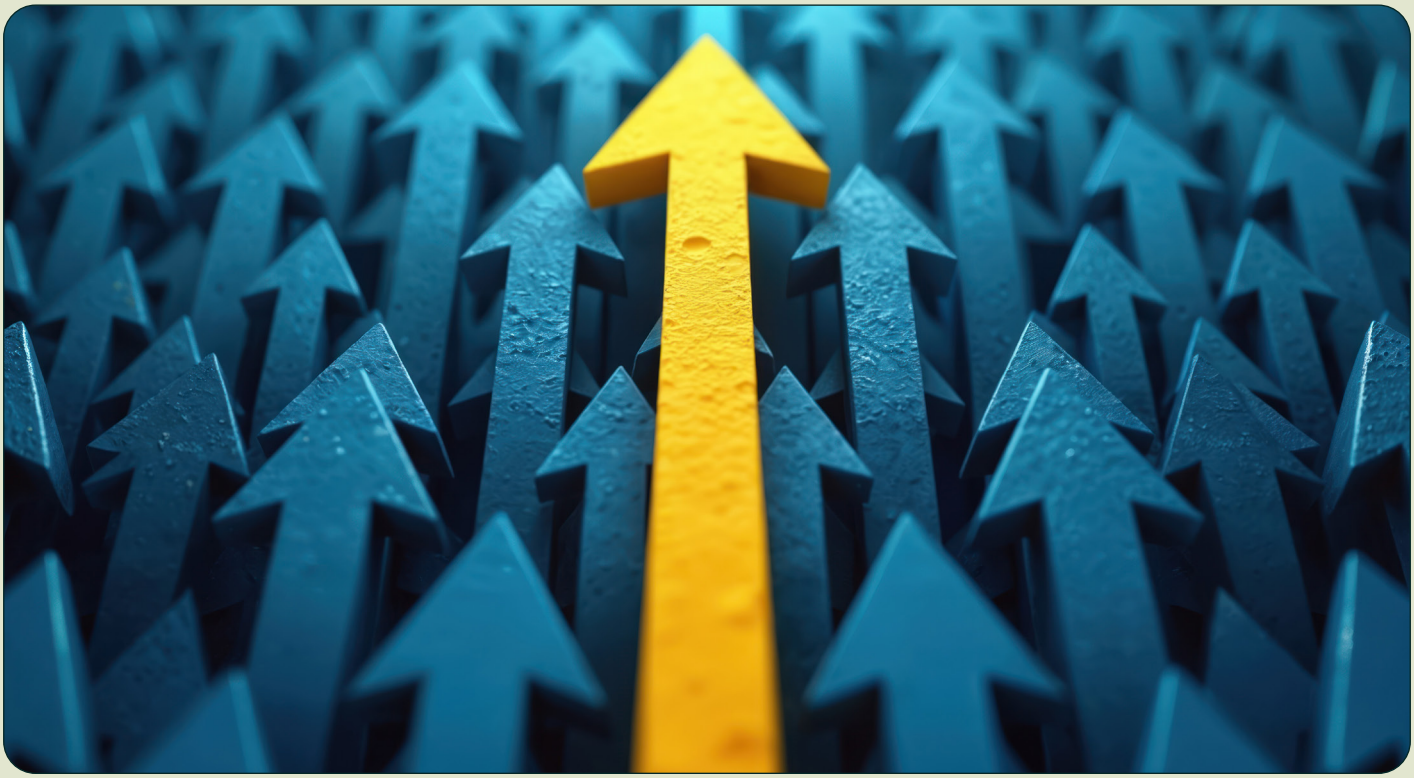
- → Safety data should follow suit. Convert metrics into consequence:
- → What was the business cost of your last near miss?
- → How much admin was spent chasing corrective actions?
- → What risk remains unresolved because of manual systems?

According to the GERI report, 84% of safety leaders don't use an integrated safety platform. That makes it harder to track patterns, respond early, and demonstrate control.

If you're still collecting incident data in spreadsheets, you're already behind – and that puts your organisation at a higher risk.

3

FRAME SAFETY AS A BUSINESS CONTINUATION TOOL.



97%

Of organisations are not future ready when It comes to safety

3%

Of organisations are future ready when It comes to safety

Cybersecurity isn't positioned as a compliance task. It's a resilience strategy.

Safety should be the same. It's not just about avoiding incidents - it's about protecting people, uptime, and performance.

Shift from:

"We need this for compliance"

to

"This reduces the likelihood of disruption and builds business continuity"

Did you know only 3% of organisations are considered future ready when it comes to safety, according to 2024 GERI Report? The rest are at risk of being caught out by manual processes, reactive thinking, or inconsistent reporting.

A future-ready safety team focuses on forward indicators, risk trends, and tools that support performance at every level of the business.

Your organisation can only achieve that with a digitised safety system.

4

PLAY IN THE GREY.

$61.8B Per Year

Workplace injuries and illnesses cost the Australian economy

= **4.8%** Per Year

Gross Domestic Product

Leverage the requirement to "do what's reasonably practicable".

When it comes to cybersecurity, companies are expected to have systems in place to protect their people, both internal and external. The same goes with health and safety.

Remind your exec team that Australian WHS law requires businesses to take all steps that are 'reasonably practicable' to ensure health and safety.

The term "reasonably" is subjective, and it's risky to leave this to chance. In the case of showing that the company is doing what's reasonably practicable, the legal risk of underinvesting outweighs the cost of a proactive approach.

A digitised safety management system can help show that reasonable steps have been taken, making it easier to demonstrate due diligence if an incident does occur.

From risk assessments and hazard controls to training records and audit trails, every step is logged, timestamped, and visible. That visibility is crucial in demonstrating due diligence to a regulator, especially in the event of a serious incident or prosecution.

Workplace injuries and illnesses cost the Australian economy an estimated **$61.8 billion annually** - around **4.8% of GDP.**

For individual businesses, that means higher insurance premiums, lost productivity, and the risk of reputational damage that's hard to undo. If you talk to these points, your board will listen.

5

USE REAL SCENARIOS, NOT HYPOTHETICALS.

Cybersecurity teams often use high impact breach stories to sell their message. Safety should do the same.

FOR EXAMPLE:
A piece of plant wasn't tagged out properly. A contractor unfamiliar with the site used it.

THE RESULT:
A crush injury, regulator investigation, shutdown of operations, and national media coverage leading to reputational damage, compensation damages, and a negative impact on profits.

Executives respond to consequence - not probability. Scenarios that reflect your own operations, your industry, or your recent close calls will be far more powerful than risk matrices or safety.

6

MAKE IT ABOUT THE BUSINESS.

"Try not to talk about health and safety. Understand their measurable. What is the exec looking for? I don't say I'm making this operation safer. I say, 'I'm making it more efficient, so it's more profitable and quicker.' The byproduct is it will also be safer."

Robert Keenan
(Safety Design & Critical Risk Lead, NZ Post)

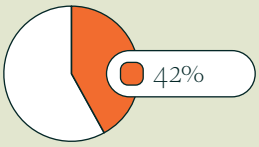
The best way to get executive buy-in? Link safety to business performance.

Show how your proposed safety initiative can:

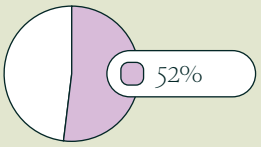
- → Reduce costs by cutting admin and duplication
- → Increase productivity by speeding up hazard response
- → Reduce downtime through proactive alerts and maintenance
- → Improve culture by embedding safety into every task

According to the GERI report, **42% of safety leaders** expect digital safety tools to reduce administrative burden. Another **52%** expect a measurable drop in incidents and injuries.

Executives want more than compliance - they want efficiency, too. **Frame your safety initiatives accordingly.**



Safety leaders who expects less admin with digital tools



Safety leaders who expects fewer incidents and injuries with digital tools

7

BUILD SUPPORT OUTSIDE THE SAFETY TEAM

"Your CEO doesn't need another compliance briefing. What they need is a strategic partner."

Dr Megan Tranter
CEO Purpose Pathfinders

Cyber leaders don't act alone. They work with finance, ops, legal, HR, and comms. They understand that budget decisions are shaped by broader input.

If you want safety to get traction, build alliances. Ask other teams:
What risks keep you up at night?
What delays or issues are caused by safety gaps?
How could a more connected safety system help your team?

When safety is seen as a shared priority - not a safety team responsibility - your influence grows.

Remember: Sell the risk, not the role.

The safety team shouldn't be selling their value. They should be showing the business risks they mitigate and the productivity they protect.

Executives understand risk. They're used to making decisions that weigh uncertainty against cost, reputation, and return.

That's how cyber earned its place at the table.

It's time that safety did too.