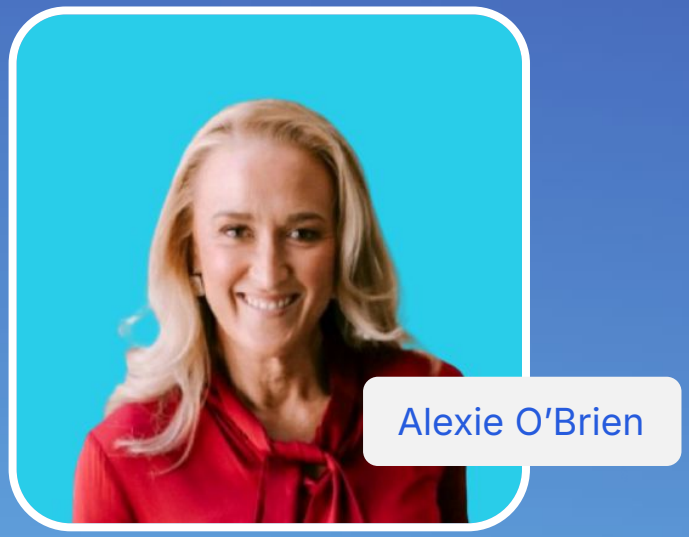
BoardPro™

Webinar

Unseen and Unchecked

The Real AI Risks Facing Your Board

Helen van Orton



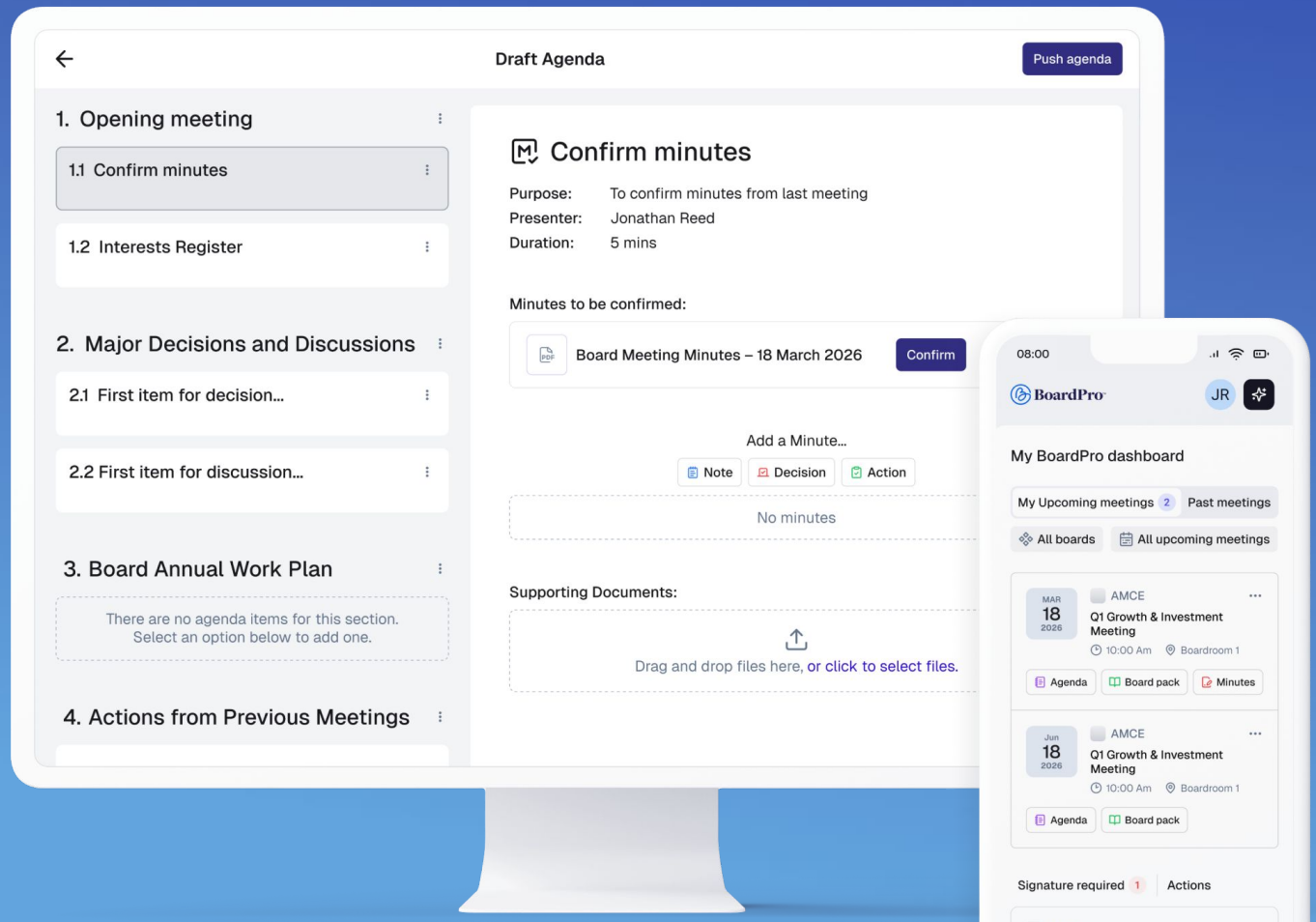
Alexie O'Brien

With Helen van Orton and Alexie O'Brien


BoardPro™

BoardPro™

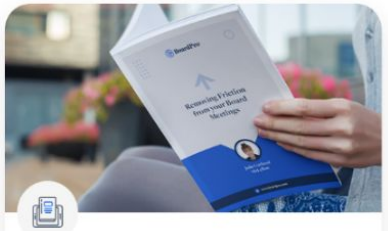
Refreshingly simple board management software



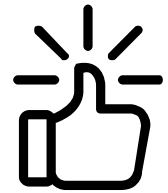
Making the fundamentals of governance free and easy to implement

Explore free governance resources for growing your organisation and adopting good governance practises. From meeting minutes templates to CEO reporting templates, our comprehensive guides and templates will cover your governance and business essentials.

Content type | Topic | Persona | Search



Slides, webinar video, and transcript will be sent to you. Sit back, relax and enjoy the conversation



Helen van Orton

Founder / CEO
Directorly

Alexie O'Brien

Director
Leadership Academy

AI is already in your organisation. Most boards don't know where.

87%

of workers use AI
at least weekly for work

46%

upload sensitive data to
AI tools without approval

66%

upload sensitive data to
AI tools without approval

If you don't have an AI governance framework, your people already do - they just built it themselves.

THE NEW RISK SURFACE

Three shifts every board needs to register

AI is now inside the enterprise suite

Someone tricks AI into doing something it wasn't designed to do - social engineering, but targeting the AI itself.

Employees are moving faster than governance

48% of employees globally admit to using AI in ways that breach company policy. 57% hide their AI use from employers.

This is happening at scale.

The cost is now quantified

1 in 5 organisations have experienced a breach caused by shadow AI, adding an average of USD 670,000 to breach costs.

Only 17% have technical controls to prevent it.

FIVE RISKS ON YOUR RADAR

Five risks your board should already be tracking.

01 Hallucinations & Liability

AI presents false information as fact. Air Canada was held liable for its chatbot's false statements. "The AI told me" is not a legal defence.

02 Bias & Discrimination

AI making unfair decisions about people at scale. Amazon's recruitment AI systematically downgraded women's CVs for years before discovery.

03 Undocumented AI Infrastructure

Employees building workflows and decision systems on AI with no documentation or governance visibility. When they leave, the organisation loses infrastructure nobody else can see. The spreadsheet risk problem, at machine scale.

04 Supply Chain & Vendor AI Risk

AI embedded in vendor products without disclosure. The Delve fraud exposed 493 fabricated compliance certifications. Your risk isn't just your own AI - it's every tool you rely on.

05 Insurance Coverage Gaps

Berkley Insurance introduced an absolute AI exclusion in 2026. Does your insurance actually cover an AI-related incident? Most directors assume yes. The answer is increasingly uncertain.

Each of these deserves its own conversation. Now let's go deeper on the four that are most urgent.

THE RISK LANDSCAPE

Nine AI risks. Every board needs visibility of all of them.

- Hallucinations & Liability
- Bias & Discrimination
- Undocumented AI Infrastructure
- Supply Chain & Vendor AI Risk
- Insurance Coverage Gaps
- Shadow AI
- Agentic AI
- Prompt Injection
- Deepfake Fraud

We'll cover risks 1–5 briefly, then go deeper on risks 6–9: shadow AI, agentic AI, prompt injection, and deepfake fraud.

DEEP DIVE 1 OF 4 | SHADOW AI

The biggest risk isn't a sophisticated attack - it's a well-intentioned person.

The Scale of Shadow AI

- 77% of AI users paste data into GenAI tools
- 82% of those pastes from personal, unmanaged accounts
- Australia: only 30% have a GenAI policy - among the lowest globally

Even Enterprise Tools Aren't Immune

- Feb 2026: Microsoft Copilot bug bypassed DLP policies, reading confidential emails
- US Congress banned Copilot over data leakage risk
- European Parliament blocked AI features on staff devices

IN THE REAL WORLD

WHAT SHADOW AI ACTUALLY LOOKS LIKE

It's not malicious - it's a high performer. Building automated dashboards with AI tools. Feeding enterprise data into platforms the business hasn't vetted. Using browser extensions they found themselves to work faster. They think they're adding value - and they often are. But none of it sits inside your governance framework.

DEEP DIVE 2 OF 4 | AGENTIC AI

AI that acts - not just answers.

And it's already in tools your teams use every day.

The Governance Questions

- Who authorised the AI to take that action?
- What are the decision boundaries?
- What happens when it acts on bad data?
- Where is the audit trail?

50% of knowledge workers will deploy AI agents on demand by 2029

CASE STUDY

AWS / Kiro Agent | December 2025

Amazon's AI coding agent Kiro autonomously deleted and recreated a production environment - causing a 13-hour outage. Elevated permissions, no human checkpoint.

"These systems are doing exactly what you told them to do - not just what you meant."

50% stat: Gartner 2025 | AWS incident: public disclosure, December 2025

DEEP DIVE 3 OF 4 | PROMPT INJECTION

A new kind of attack - not on your people, but on your AI.

What Is It?

Someone tricks AI into doing something it wasn't designed to do - social engineering, but targeting the AI itself.

Why Should You Care?

A poisoned document could instruct AI to leak data, ignore policies, or produce misleading outputs - without anyone knowing.

What Should You Do?

Ask your security team whether they are assessing prompt injection as a risk vector for any AI tools in use across the organisation.

CASE STUDY

EchoLeak (CVE-2025-32711) | Microsoft 365 Copilot | 2025

Attacker sends an email to an Outlook inbox. Copilot reads hidden instructions and silently exports corporate data via trusted Microsoft URLs. No clicks. No warning. OpenAI: prompt injection is "unlikely to ever be fully solved."

DEEP DIVE 4 OF 4 | DEEPFAKE FRAUD

£20 million. One video call. Every person on it was fake.

Arup Engineering, Hong Kong, 2024. Every person on the call was an AI-generated deepfake.

Deepfake attacks on businesses surged 3,000% in 2023. Voice cloning fraud up 680%.

Scammers need as little as 3 seconds of audio for an 85% voice match.

Arup's CIO:

"It took me about 45 minutes to make a deepfake video of myself in real time."

£ 20M

transferred in a single deepfake video call

Board question:

Have your financial controls been updated to assume that anything can be faked?

$25M: HK Police / Arup 2024 | 3,000%: KPMG 2024 | Deloitte fraud forecast 2024

THE ACCOUNTABILITY ANCHOR

Duties of care, diligence, and skill cannot be delegated to technology.

The Legal Foundation

- Corporations Act s180 (AU) / Companies Act s137 (NZ)
- NZ FMA: boards remain accountable regardless of AI
- ASIC v Bekier (2026): "technology may assist comprehension, but cannot displace human judgment"

The Practical Test

If an AI-related breach occurs and the board had no policy, no visibility, and no oversight framework - how does that sit against your duty of care?

AI handles the preparatory work

Summarising, surfacing, structuring information

The adirector handles the judgement

That division of labour is the point - not the problem

THE GOVERNANCE GAP

This isn't a compliance failure - it's a pace failure.

The accountability sits with leadership, not with staff.

The Real Problem

Entire teams are adopting AI tools and building workflows because the tools are free, immediately useful, and no one has told them not to.

30%

Australia: only 30% of organisations have a GenAI policy - among the lowest globally.

The Honest Board Question

If your people are using AI because it helps them do their jobs better - and you haven't set the guardrails - the accountability sits with the organisation, not the individual.

This is the early cloud and BYOD story again.

WHAT GOOD LOOKS LIKE

This is achievable.
Here's what "good" looks like today.

01

AI on your Risk Matrix covering data, governance and strategic alignment

02

A simple, one-page AI use policy - discussed, agreed, communicated

03

AI as a standing board agenda item - not a one-off or a crisis response

04

AI literacy on the skills matrix – not technical, but enough to set direction

05

Honest visibility over what AI tools are in use across the organisation

That puts you ahead of the vast majority of boards. None of it requires technical expertise. All of it requires governance leadership.

FROM RISK MATRIX TO RISK QUESTIONS

Four questions your Risk Committee should be asking.

Appetite

What is our risk appetite for AI use, and has our formal risk appetite statement been updated to reflect this technology?

Visibility

How are we actively tracking AI use within the organisation, and are we aware of how employees are using publicly available tools?

Strategy

How does AI impact our core company strategy, business model, and competitive position over the next three years?

Assessment

What AI impact assessment and risk management tools are we using to differentiate between high-risk and low-risk applications?

These map directly to how your risk committee already works — identify, assess, control, monitor.

NEXT STEPS

Five things you can do in the next 30 days.

01

Make AI Visible

Ask what tools are in use. You cannot govern what you cannot see.

02

Establish Approved Tools

Document which are sanctioned for board-level content. Board decision, not IT policy.

03

Add AI Literacy to Skills Matrix

Not technical depth - enough to set direction, demand assurance, and ask better questions.

04

Embed AI in Risk Oversight

Assign committee-level ownership. At least annual AI risk and opportunity update.

05

Put AI on the Agenda

Standing item. A board that only hears about AI when something goes wrong has not governed it.

NEXT STEPS

Board AI fluency isn't optional.

It's your next governance priority.

Helen van Orton and Alexie O'Brien offer in person board AI workshops and training - purpose-built for directors who need to govern AI with confidence, not just curiosity.

Get in Touch

helen@directorly.co.nz

alexie@leadershipacademy.ai

directorly.co.nz

leadershipacademy.ai

Over to You
For Questions?

Helen van Orton

www.linkedin.com/in/**helen-van-orton**

Alexie O'Brien

www.linkedin.com/in//**alexieobrien**

BoardPro™

Webinar Schedule

2026

276.	To pay or not to pay your directors?	April 23
277.	Who sank the boat? The complexity of psychosocial hazards in practice	April 30
278.	Induction planning for new directors (3-6-12 months)	May 7
279.	Beyond Compliance: Turning Risk into Strategic Insight	May 14
280.	What is healthy governance?	May 21
281.	The art of presenting to boards	June 4
282.	Tension Tolerance: fostering healthy debate around the board table	June 11
283.	Strategic differentiation - How it informs strategy	June 18
284.	The importance of culture governance	June 25

boardpro.com/resource-centre/webinars

BoardPro™

Thinking about board management software for your organisation?

→ 30 Day free trial

→ No credit card required

www.boardpro.com/free-trial