IMAP MDA Webinar Series

Insurance for MDAs

Stephen Hughes, AJ Gallagher
Jesse Vermiglio, Holley Nethercote

IMAP
Institute of Managed Account Professionals

MDA 360 Program

	MDA Webinar series
17th August	Insurance for MDAs
18th August	Understanding your Fiduciary Duty as an MDA Provider
19th August	Identifying and Managing Conflicts of Interest
20th August	Fee disclosure for MDAs
21st August	Shifting Ground: Strategic Challenges in Managed accounts for Advisers
	MDA Masterclasses
28th October	Best Practice Advice using an MDA Service
18th November	Responsible Manager for MDA
9th December	Risk Management for MDA Risks
19-20 November	**MDA Leadership Summit**

MDA Subscribers discount

MDA 360 Program

	Presenters
AJ Gallagher	**Steven Hughes** – Principal
Akambo	**Jane Zhou** – Head of Governance
Consultant	**Mark Watmore**
Crowe	**Sean Pascoe** – Partner
JM GRC Consulting	**Jenny Mulders** - Founder
Hamilton Locke	**Simon Carrodus** – Partner
	Jaime Lumsden – Partner
Holley Nethercote	**Michael Mavromatis** – Partner
	Jesse Vermiglio – Partner
HSF Kramer	**Andrew Bradley** – Partner

Jesse Vermiglio

Holley Nethercote

HOLLEY NETHERCOTE

MDAs and PI insurance

Institute of Managed Account Professionals

17 August 2026

MDAs and PI insurance

- Why PI insurance is required
- MDA providers and Advisers: different PI insurance requirements
- Nature of MDA regulation
- Risks of MDAs
- Key take-outs

PI requirements: MDA providers versus advisers

	MDA providers	Advisers
Source of obligations	ASIC legislative instrument: s912AED notionally inserted.	• s912B Corps Act • reg 7.6.02AAA
Reg Guides	RG 179	RG 126
Coverage	**Adequate** having regard to the nature of the activities carried out by the licensee in relation to MDA services.	**Adequate** taking account certain factors in the regs.
Minimum cover	Lesser of: • **$5m;** or • Aggregated average value of client portfolio assets of all people to whom MDA service retail clients in previous 12 months.	At least: • **$2m;** or • total revenue from financial services provided to retail clients up to $20 million (actual or expected revenue).
Whose losses is it meant to cover	**Retail client losses**	**Retail client losses**

PI requirements: MDA providers versus advisers

	MDA providers	Advisers
Specific cover	PI cover incl cover for fraud by its officers and employees.	Min requirements for loss or damage because of breaches of Ch 7 (incl fraud or dishonesty by officers and employees) and AFCA awards.
Exclusions	Silent	Policy must not have certain exclusions.
Automatic reinstatements	Silent	At least one reinstatement.
Excess/deductible	Silent	Can be sustained as uninsured loss.
Defence costs	Silent	Must be in additional.
Retroactive cover	Silent	Yes

Key aspects of MDA regulation

- Tailored requirements within the broader AFSL regime
- Why retail MDAs are treated differently to wholesale MDAs
- Relief from various Corps Act requirements
- Enhanced disclosure requirements
- Upfront and ongoing obligations about suitability of MDAs
- Separate breach reporting regime

Risks of operating / advising on MDAs

- Wholesale client versus retail clients
- Suitability of MDAs
- Conflicts of interests
- Investments not in line with Investment Program
- Fee Disclosure
- High risk strategies
- Outsourcing
- Administration errors
- AI and Cyber incidents

HOLLEY NETHERCOTE

Key take-outs

1. Read your PI insurance policy
2. Know what services you provide in relation to MDAs
3. Know the risks of providing those services
4. Have an effective compliance framework to respond to such risks
5. Regularly review your PI insurance cover

HOLLEY NETHERCOTE

Stephen Hughes
AJ Gallagher

Managed Discretionary Accounts (MDA)

- Professional Indemnity and Cyber liability risk exposures

Case Study

- MDA claims often involve multiple allegations

Husband and wife – professionals with high income who held their super through industry super funds. Recommendation – establish an SMSF and invest through an MDA. Adviser sent wholesale letter to clients to sign. Alleged adviser said 'nothing will change' it will merely reduce paperwork / compliance burden. No accountants certificate provided nor renewed after 2 years.

The complaint alleges that: AFSL operated portfolios through an MDA service;

portfolio rebalancing occurred over several years;

there was a substantial increase in international equity exposure;

the clients did not fully understand the risk profile being created;

And the wholesale classification reduced the disclosure and explanation they would otherwise have received as retail clients.

Key point: Retail v Wholesale – funds held in an SMSF (Product value test only wholesale client if net assets in super >$10m)

The issue is not AFCA's Compensation cap, but rather that MDA disputes often involve an entire portfolio over many years, allowing alleged losses to accumulate into hundreds of thousands or even millions of dollars before AFCA assesses causation and compensation. My experience with claims against traditional advisers is that the EDR scheme will look at a particular investment in isolation. For instance when Basis Capital collapsed they considered that in isolation against other investments in the portfolio. So whilst a portfolio may have increased in value there was still compensation payable. In an MDA complaint AFCA may effectively review years of discretionary investment decisions, portfolio rebalancing, governance particularly where the suitability is in question.

AFCA case study – leveraged FX

- Determination in favour of the client

The client held an SMSF, was placed into a leveraged FX strategy which resulted in significant losses. AFCA found that the client had been incorrectly classified as a wholesale rather than a retail investor

- Client classification failures
- High risk investment strategies
- Suitability concerns
- Breach of regulatory obligations

Key issue: incorrect classification can significantly increase claim severity

MDA exposure v PI portfolio response

Exposure	Typical alllegation	PI Coverage
Wholesale Client Classification	Incorrect wholesale categorisation	Usually covered but can create very large claims
Approved Product List (APL)	Product not approved or approval process not followed	APL Exclusion
Conflict of Interest	Adviser benefits from recommendation	Conflict of Interest Exclusion
Related Party Investments	Lack of independence	Related Party Exclusions
Leveraged / High Risk Investments	FX, derivatives, CFDs, concentrated positions	Financial Institution / High Risk Investment Exclusions
Portfolio Drift	Failure to monitor or rebalance	Usually covered negligence claim
Investment Mandate Breach	Investments outside agreed strategy	Coverage generally available unless deliberate conduct
Outsourcing	Third party manager error	Outsourcing / agency issues
Trading Errors	Unauthorised trades	Usually covered subject to circumstances
Multi-year Portfolio Management	Issues developing over many years	Retroactive Date / Continuous Cover concerns

The Cyber Threat Landscape

The current state of Australian Cyber Risk

95% of cyber claims caused by human error

Key Statistics from the ACSC's FY23 Threat Report

OVER 76,000 INCIDENTS
A 13% increase since FY21

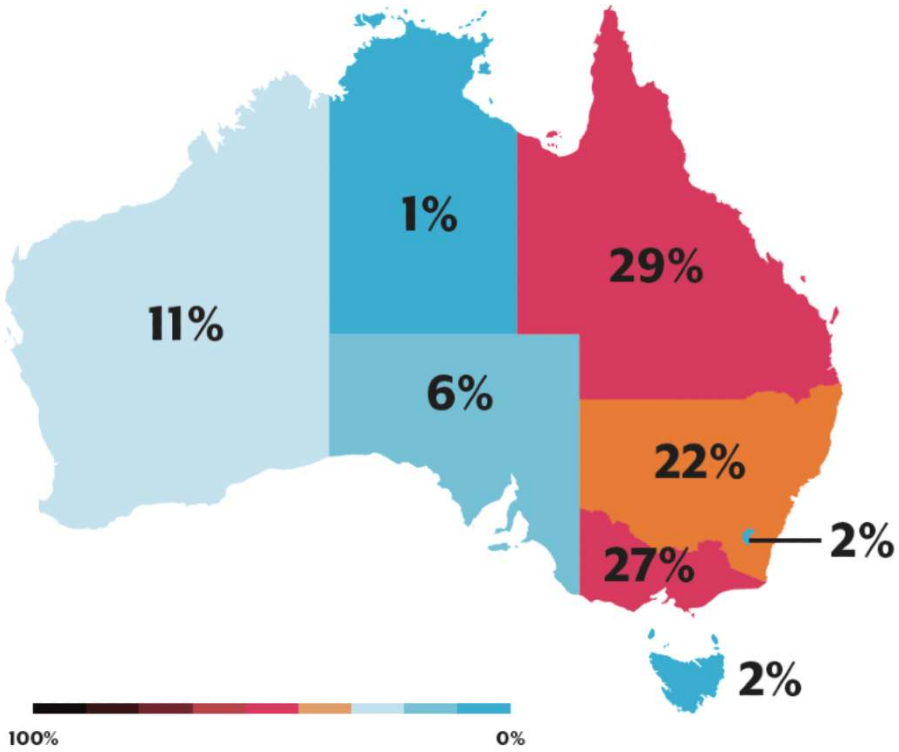
1 CALL EVERY 7 MINUTES
20% more calls to 1300 CYBER1 hotline than FY21

NOBODY IS IMMUNE
Australia's East Coast made up 80% of all reported incidents

$33 BILLION IN DAMAGES
The figure of self-reported losses

INCREASING BY THE DAY
15% increase in Cybercrime efforts in FY22

SOFTWARE VULNERABILITIES ON THE RISE
25% increase in Common Vulnerabilities and Exposures (CVEs)

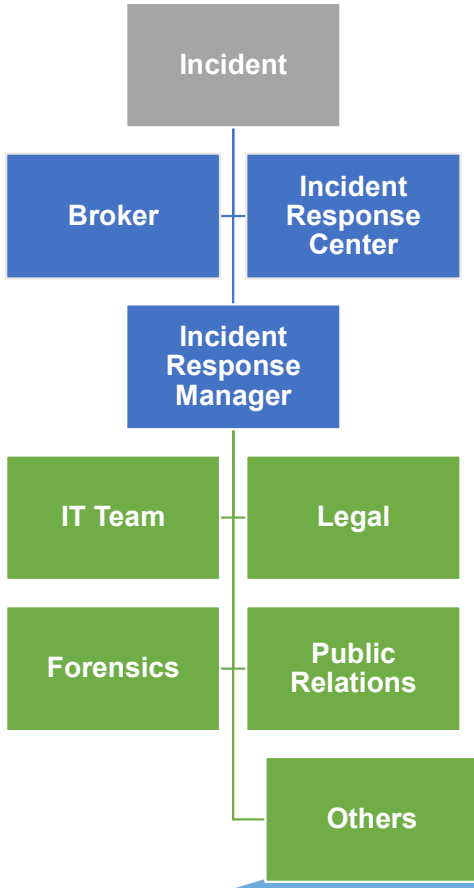


Incident Response Process

As part of a Cyber insurance policy, Insured's have access to a cyber-incident response hotline where an assigned Incident Response Manager will coordinate the response and deploy specialist resources on the insurer's vendor panel to help mitigate further loss and assist clients with returning to 'business as usual'.

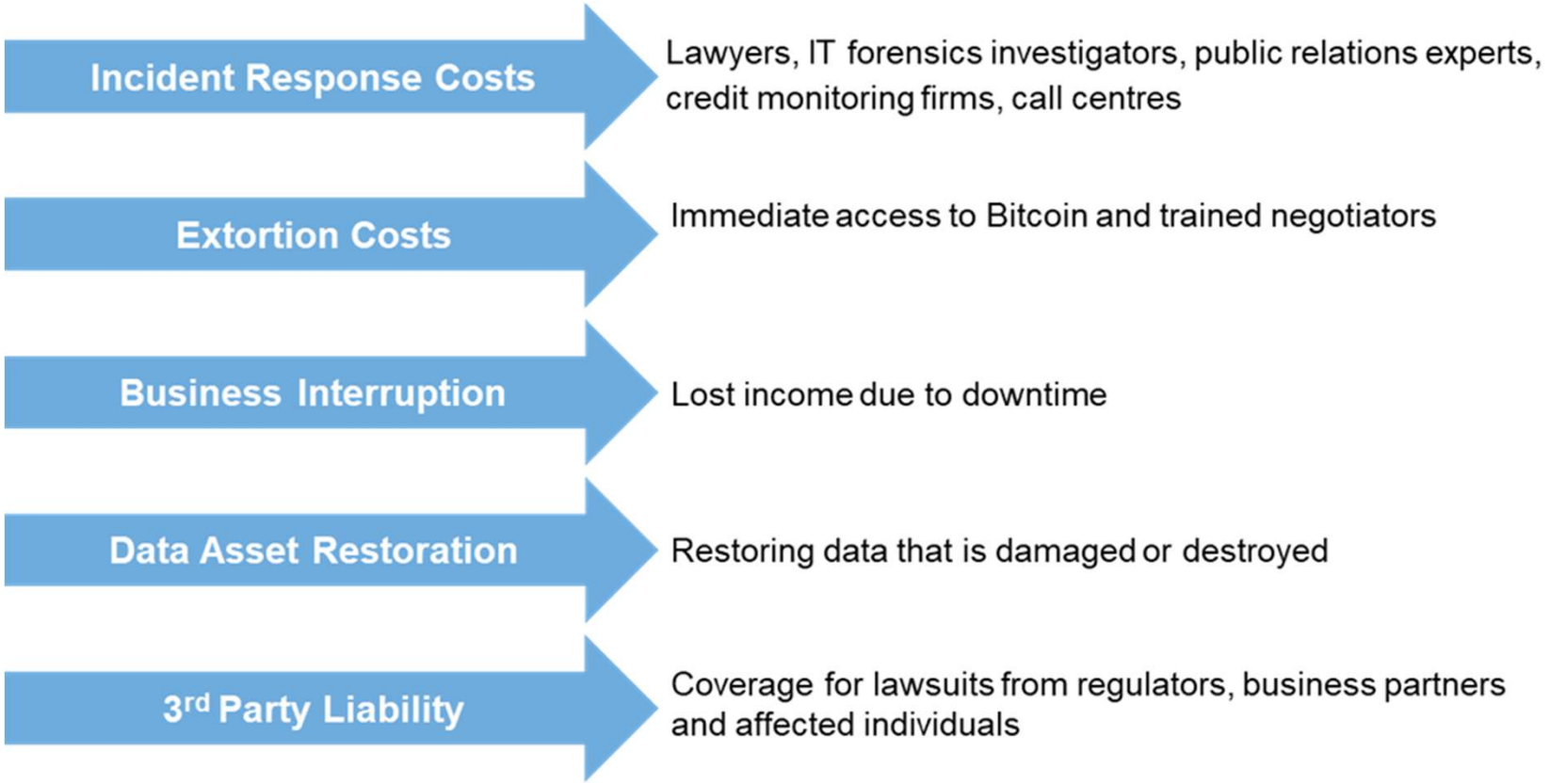
Key Question:
Did the incident expose a weakness that caused, or is likely to cause, a significant breach of our AFSL conditions?

Must report within 30 days



Cyber Security Insurance

What is covered?



The Role of the Privacy Commissioner

Notifiable Data Breaches Scheme

A common misconception is that businesses with an annual turnover under $3 million are exempt from the Privacy Act. This is not true. You must comply with the Act if you handle sensitive personal information, such as Tax File Numbers (TFNs), and you are required to notify the Australian Information and Privacy Commissioner (OAIC) of an "eligible data breach".

Eligible breach examples:

- Personal information is accessed without authorisation, disclosed or lost and a reasonable person would conclude the incident is likely to result in serious harm.

Australian Government

Office of the Australian Information Commissioner

• General Impact of Cyber Events

- **Privacy Commissioner Investigation**: Businesses may face investigations by the Privacy Commissioner, which could result in fines and penalties for the release of sensitive data.
- **Accountability for Data Breaches**: Businesses are held accountable for the release of sensitive data, even if they outsource IT services or use cloud providers.

RI Advice

ASIC v RI Advice Group (2022)

The Federal Court found that RI Advice breached its AFSL obligations by failing to maintain adequate cybersecurity risk management systems across its authorised representative network.

The Court made it clear that **cyber resilience is a core governance, risk management and AFSL compliance issue, not merely an IT function**. RI Advice was ordered to implement further cyber controls with the assistance of an independent cybersecurity expert and pay **$750,000 towards ASIC's legal costs**.

Key Message for AFSLs and MDA Operators

- **Key Question**:

Did the incident expose a weakness that caused, or is likely to cause, a significant breach of our AFSL conditions?

Must report within 30 days

Poor cybersecurity can itself constitute a breach of AFSL obligations. ASIC expects licensees to maintain appropriate cyber risk management frameworks, oversee authorised representatives and service providers, and implement controls capable of protecting client information and financial services operations.

Emerging risk -Artificial Intelligence

The Next Governance Challenge. What is changing?

Traditional software follows instructions.

Agentic AI systems can make decisions, initiate actions and interact with other systems with limited human intervention.

Financial services firms are increasingly exploring AI for:

- Portfolio monitoring
- Client communications
- Research and analysis
- Trade recommendations
- Workflow automation
- Compliance monitoring

Steps in the Claim Process

I. Immediate Reporting:

A. The insured must immediately contact the the incident response team for the insurer. Details and circumstances of the event must be provided.

II. Assessment and Investigation:

A. The Insurer assesses whether the claim is covered under the policy.

B. A forensic investigator may be appointed to determine the extent of the incident and its root cause.

III. Incident Response Team Deployment:

A. A breach coach is appointed to coordinate the response.
B. IT forensic experts investigate and secure the environment, identify vulnerabilities, and provide remediation advice.
C. Legal counsel advises on privacy obligations and regulatory requirements.
D. Crisis communication experts manage media and stakeholder communications to minimise reputational damage.

IV. Threat Actor Engagement:

A. Ransom negotiators engage with the threat actor to negotiate the ransom amount, ensure compliance with sanctions, and secure a decryptor if necessary

V. IT systems are restored, and data recovery is initiated.

VI. The insured is guided through the process to return to "business as usual."

MDA 360 Program

	MDA Webinar series
17th August	Insurance for MDAs
18th August	Understanding your Fiduciary Duty as an MDA Provider
19th August	Identifying and Managing Conflicts of Interest
20th August	Fee disclosure for MDAs
21st August	Shifting Ground: Strategic Challenges in Managed accounts for Advisers
	MDA Masterclasses
28th October	Best Practice Advice using an MDA Service
18th November	Responsible Manager for MDA
9th December	Risk Management for MDA Risks
19-20 November	**MDA Leadership Summit**

MDA Subscribers discount