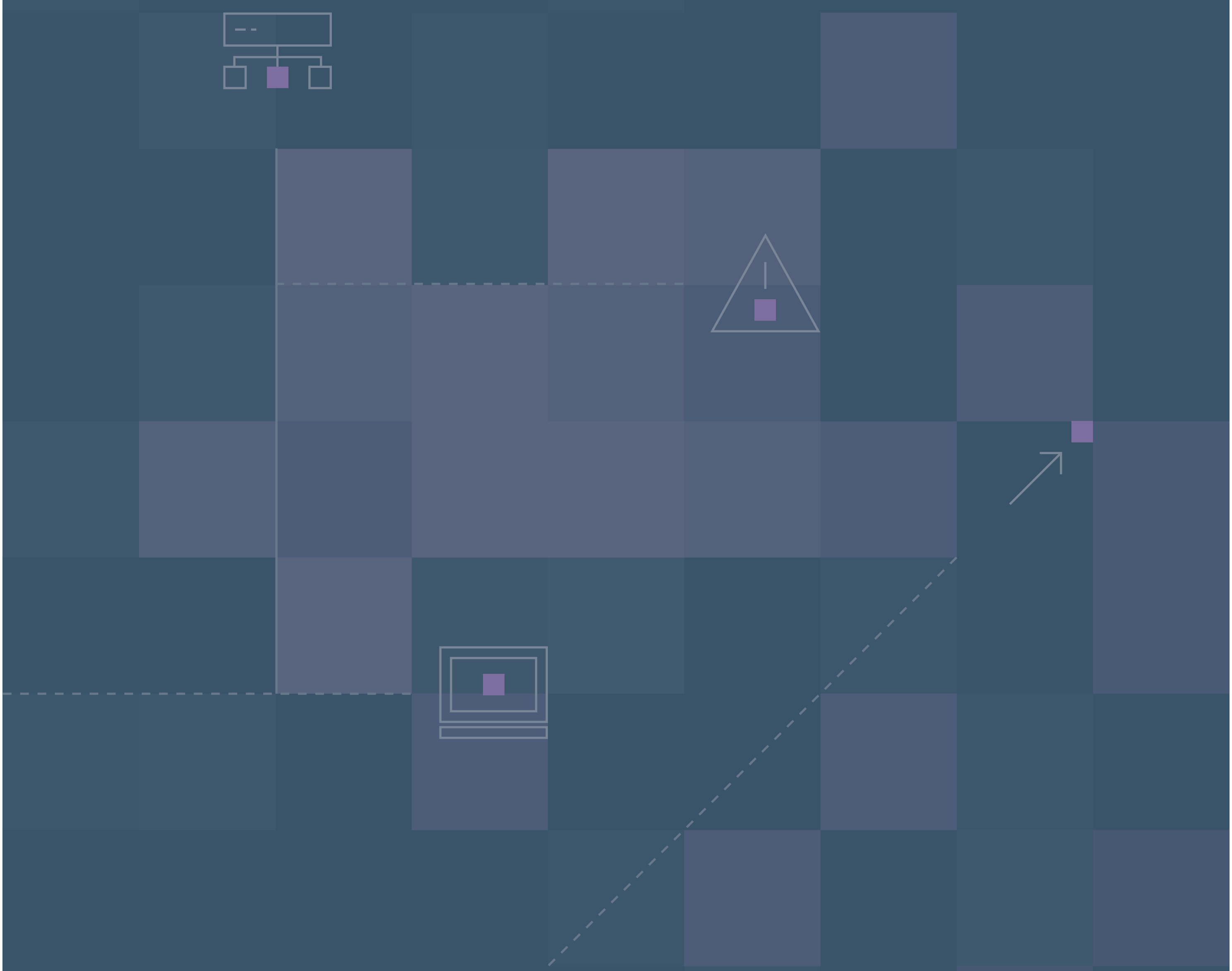
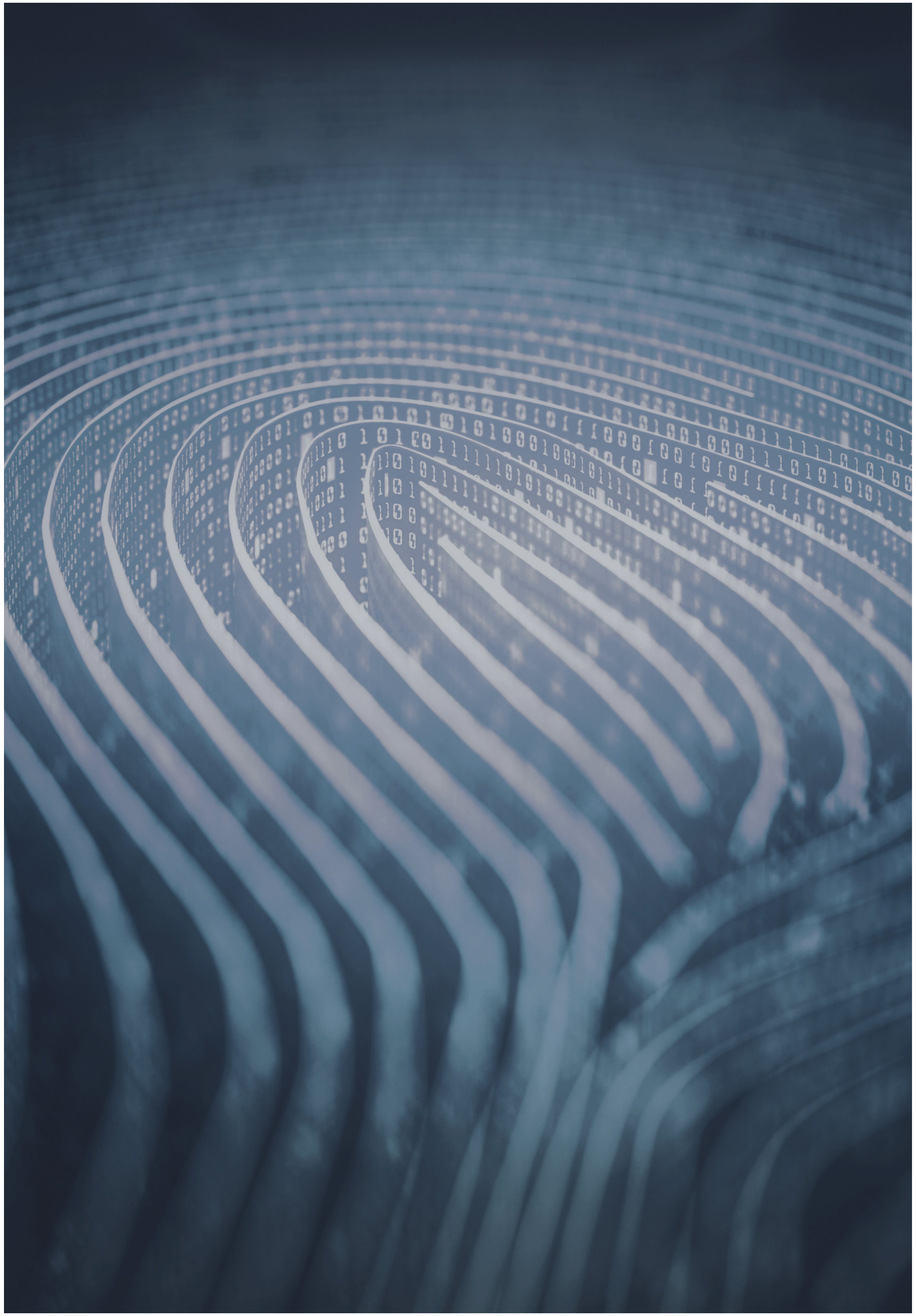
KordaMentha



Cybersecurity solutions

Managing your business risk
and responding to cyber incidents.

kordamentha.com



Cybersecurity solutions

Managing your business risk and responding to cyber incidents.

Cybercrime has become one of the biggest threats to business viability worldwide and is now consistently among organisations' key enterprise risks. The damage may be far reaching, from financial and intellectual property losses to reputational damage, and may hinder client relationships and future growth. With mandatory data breach reporting obligations and increasing regulatory pressure, business leaders must draw on specialist expertise to mitigate risks and minimise losses.

KordaMentha's cybersecurity specialists work with boards, executives and organisations to evaluate their risk, develop mitigation strategies and implement solutions. We assist organisations to manage their cyber risk effectively with the design and adoption of strong governance, operating models and risk reporting frameworks. Incorporating security compliance requirements into our approach also assists our clients to enhance their consumer and business partner confidence.

Clients rely on our cyber response experts to maintain business operations and minimise impacts following a cyber incident. Drawing on our broad range of incident response and digital forensic professionals, we assemble a team with the right expertise for each engagement. This allows us to provide a rapid, action-orientated and outcome-driven response at a time when inaction can be costly and lead to further loss. When required, we can adapt our approach from incident response to a detailed digital forensic investigation, potentially complemented by eDiscovery, financial impact quantification and expert witness assistance.

How we can help you

Security risk, maturity and compliance assessments

We provide a holistic cybersecurity assessment against risk or industry-leading security standards to verify the posture and risk exposure and ensure that improvements needed to safeguard data are clearly defined and aligned to the organisation's target state. We help c-suite and board members understand the organisation's cybersecurity position and how they are meeting regulatory or specific industry requirements.
Our assessments include, but are not limited to:

- Detecting, evaluating and prioritising risks to organisational reputation, information, assets, operations and employees.
- Identifying compliance with security standards, regulations and government standards.
- Identifying risks posed by third-party connections in the supply chain.
- Effectiveness and maturity assessment of vendors' cybersecurity controls.

Cybersecurity strategy, governance and advisory

We work with organisations to implement evidence-based security roadmaps to achieve their target cybersecurity posture. KordaMentha develops cyber strategy, operating models and compliance management programs. We also collaborate with clients to manage the organisation's cybersecurity risk and program. Our services include:

- Development of comprehensive security strategy tailored to an organisation's objectives and obligations.
- Development of an operating model and cyber risk reporting framework.
- Compliance management against specific security standards or regulations.
- Security management or CISO-as-a-service.

Cybersecurity training

Employees play a critical role in an organisation's cybersecurity defence. It is vital that people within the organisation are educated and confident when it comes to cybersecurity. We help clients prepare for critical incidents and educate them on how to respond effectively, should one occur. This may include:

- Cybersecurity education and awareness training.
- Technical tabletop exercises.
- Board/Executive breach simulation.

Response planning and testing

KordaMentha develops proactive incident response programs that position an organisation to effectively manage a security breach. We review existing incident response policies, plans and playbooks, and conduct interviews with relevant stakeholders. This allows us to understand the organisation's people, processes and technology, and develop a program that prepares the organisation for cybersecurity incidents. This can include:

- Incident response plan development or assessment.
- Incident response plan stress testing and playbook development.
- Security framework/policy review and development.

Incident response

Our rapid response immediately contains an incident, identifying the point of breach and working with clients to ensure the vulnerability is remedied. We help clients understand the incident's lifecycle, focusing on initial control weakness that facilitated the incident through to the trail of compromised systems and data. This includes:

- Collecting relevant data in the immediate aftermath of an incident.
- Utilising KordaMentha's cybersecurity lab infrastructure to securely process and analyse data.
- Determining the extent of any unauthorised access and/or data exposure.
- Conducting data exfiltration and impact analysis review.
- Providing a summary report which details the findings of the incident response investigation.
- Making a formal presentation to the board or key stakeholders.

Expert reporting, litigation support, eDiscovery and financial loss quantification

KordaMentha's accredited digital forensics professionals conduct detailed and thorough investigations, analysing the underlying facts and circumstances. With our extensive in-court experience, we understand the risk and pain points in managing incident response investigations from data collections through to any formal reporting requirements. Our experts are often called upon to provide oral and written testimony to ensure the investigation is robust and defensible and will withstand scrutiny.

Our eDiscovery experts help identifying and collecting relevant electronic information from immense quantities of data for use as evidence in investigations and legal cases. If a cyber attack causes financial loss, our forensic accounting specialists can be appointed to quantify the loss resulting from the attack or network interruption. Our specialists identify and develop key financial information suitable for the submission of damages measurement.

Our experience

Protecting critical health information

Background

Our client was a high-profile healthcare provider seeking assistance with managing their cybersecurity risk to protect client information and mitigate both reputational and financial risks. KordaMentha was engaged to conduct an initial cybersecurity capability assessment of the client's current security posture and identify any areas requiring improvement.

Our approach

As part of our on-site audit, we conducted interviews with key stakeholders from across the organisation, including responsible executives, the head of IT and the outsourced IT service provider. We also performed a review of the organisation's policies and documentation, a technical review of its Microsoft Office 365 environment and an assessment of the security measures implemented and managed by its IT service provider. Our findings were reported using the ACSC Essential Eight Maturity Model, a standard recommended by the Australian Federal Government.

As well as presenting the findings of our assessment to the Board of Directors, KordaMentha provided a formal report which detailed our findings and recommendations regarding identified gaps. The report also provided a clear and prioritised roadmap that allowed the organisation to commence a security uplift that will reduce its current cybersecurity risk to an acceptable level.

Outcomes and benefits delivered

- We reviewed the security capabilities and maturity of a high-profile healthcare organisation, its key technical systems and its IT service provider.
- We provided insight into our client's business security risk and provided a clear, prioritised list of key recommendations, allowing them to remediate this risk to an acceptable level.

Misconfigured cloud storage results in data leak

Background

Our client became aware of a data breach disclosing highly sensitive customer information. The client used a commercial storage solution to share and exchange data internally and externally with authorised clients. Due to a misconfiguration made by untrained and inexperienced members of the internal IT team, extremely sensitive client data was inadvertently exposed and made publicly available. KordaMentha was engaged to provide independent support to the board and executive team in identifying and quantifying the level of exposure the business had because of the incident.

Our approach

The client was a multi-national with multiple global clients (including government). One of our challenges was differentiating legitimate access to the exposed data and access by unknown and possibly malicious actors. Implementing our cyber breach workflow, we identified and engaged with the key stakeholders to obtain relevant information, isolate the breach and commence analysis. Leveraging our data analytics tools, we extracted and reviewed over 16 million log entries to pinpoint the unauthorised access.

We assessed the nature of files subject to unauthorised access and investigated whether partially downloaded files might also have exposed confidential client and company information. Our team conducted a forensic analysis of several partially downloaded file types, which included zip files. We further leveraged the power of our document review platform, RelativityOne, to enable client review and categorisation of the sensitivity of potentially exposed documents.

The results of our analysis equipped us to clarify our client's level of exposure risk to the executive team. Our findings were then provided in an expert report to the legal team.

Outcomes and benefits delivered

- We identified the source and scale of the leak and the nature of documents accessed, including partial leaks where files were incompletely exposed.
- We assisted the business in managing its obligations under the mandatory data breach legislation.

What makes us different?

We take an enterprise-wide approach to cybersecurity for our clients.

We are experts in helping organisations manage risk when the stakes are high. Cybersecurity is a critical enterprise risk for all organisations that goes well beyond technology platforms and systems into to the heart of an organisation's strategic and operational ambitions. Our specialised team of cybersecurity experts have deep experience in helping organisations manage their cybersecurity risk and respond to incidents.

Our multidisciplinary expertise

We are experts in cyber risk, incident response and organisational strategy compliance and reporting. Our specialists also have vast experience helping clients with mitigating and minimising both financial and reputational losses.

Our business focused approach

KordaMentha has extensive experience working with boards and c-suite professionals. We work with our clients to address issues and develop plans for risk mitigation, partnering with internal teams to implement the best approach. We balance stakeholder management, time sensitivities and cost.

Robust credentials

Our certified professionals have the capability and experience to assist with incident response planning and testing, and rapid delivery of an incident response service to immediately protect and recover value at risk. We partner with a range of organisations, including the Australian Cyber Security Centre, ensuring we have access to the latest threat intelligence and incident response technology.

Security is paramount

Our team also has extensive experience in investigations, digital forensics, eDiscovery and data recovery, which can help clients mitigate recovery risks, understand what happened, secure evidence and support internal, legal, regulatory and law enforcement inquiries. Our data collection and data preservation experts follow a strict chain-of-custody protocol in accordance with best practice guidelines, including the HB-171 Australian Standards guideline on the collection of electronic evidence.

How we work with clients

We assist clients with proactive cybersecurity risk identification and management, including incident response planning and testing. Should a cyber incident occur, our experts work rapidly to protect and recover value at risk.

Identifying your risk

Undetected risks can leave organisations vulnerable to cyber attacks and data breaches which can lead to financial and reputational losses. KordaMentha helps clients understand their organisational cyber risk relating to information, people, process and technology. We then work with our clients to understand their risk appetite and risk tolerance, consider the effectiveness of existing controls and identify gaps.

Managing your risk

KordaMentha helps clients proactively manage their cybersecurity risk and meet security compliance obligations. We assist organisations with the definition and implementation of security strategies or roadmaps, security operating models and reporting structures, meeting legal, regulatory and supply chain compliance requirements and ongoing cybersecurity risk management (CISO-as-a-service).

Preparing and testing your incident response plan

KordaMentha delivers proactive incident preparedness assessments, plans and testing that help clients develop and enhance their incident response programs, laying the groundwork for successful incident response and recovery. We help clients prepare for cybersecurity incidents and educate them on how to respond effectively, should a cybersecurity incident occur.

Helping you to respond to an incident

KordaMentha's certified and experienced incident response team deploys rapidly to protect our clients in the event of a breach. Once the threat is secured and business continuity is achieved, we conduct detailed investigations, ensuring the breach vector cannot be further exploited. KordaMentha can also provide in-depth forensic analysis to determine how and why the incident occurred, or eDiscovery to identify and deliver electronic information as part of an investigation. Forensic analysis and expert reporting may assist with legal, cyber insurance, regulatory or law enforcement obligations.

Key contacts

Brendan Read Partner | Brisbane

Brendan's two decades of forensic technology and investigations experience includes 10 years with the Queensland Police Service. A founding member of the High-Tech Crime Investigation Unit, he worked with State, Federal and International law enforcement agencies, including the US Secret Service, co-ordinating multi-jurisdictional investigations into fraud and cyber related criminal activity. Brendan has led complex cyber incident responses and has given evidence in many matters before courts and in civil proceedings.

+61 7 3338 0254 | bread@kordamentha.com

Catherine Lee Partner | Singapore

Catherine's attention to detail and honest communication style, combined with her project management and technical skills, helps clients in crisis. Catherine has over 20 years of experience in providing forensic investigative and advisory services to clients across diverse industries including technology, manufacturing, retail & consumer and finance institutions in the United States of America, China, and Southeast Asia. She specialises in digital forensics, eDiscovery, fraud, regulatory, and foreign bribery investigations, and litigation support. Catherine understands the time sensitivity involved when clients face difficult situations and helps clients deal with such issues efficiently by utilising technology to uncover facts.

+65 6593 9324 | clee@kordamentha.com

Ian Simpson Director | Brisbane

Ian has 23 years' experience in information technology, including security related roles. He helps clients implement security controls and frameworks in a pragmatic fashion, contextually aligned to the organisation's strategy, operating model, and threat environment. Ian is a member of the Information Systems Audit and Control Association and holds certification in the Governance of Enterprise IT, as an Information Security Manager, and as a Lead Auditor in ISO/IEC 27001:2013.

+61 7 3338 0257 | ian.simpson@kordamentha.com

Peter Chapman Partner | Sydney

Specialising in the fields of forensic technology, cybersecurity and electronic discovery, Peter has more than 20 years of experience in technology incident analysis and investigation. Peter has conducted hundreds of investigations and review projects for matters involving intellectual property theft, fraud, regulatory response, computer crime, IT security incident analysis, IT project failure and system activity analysis for government and corporate clients, including multi-national financial institutions.

+61 2 8257 3035 | peter.chapman@kordamentha.com

Tony Vizza Executive Director | Sydney

Tony has over 20 years of experience assisting organisations manage information technology and cybersecurity risk. Having worked across the globe with government, industry and academia stakeholders, he brings extensive expertise in the areas of IT, cybersecurity, privacy and the law. With board and senior management experience, Tony assists organisations to optimise their cybersecurity risk management strategies, helping convert their cybersecurity challenges and concerns into strengths and devising strategies to reduce risk, optimise operations and promote cyber resilience.

+61 2 8257 3032 | tvizza@kordamentha.com

Paul Harrison Director | Melbourne

With a strong interest in all forms of digital forensics, Paul has led an accomplished career working in all areas of digital forensics including device, cloud, document, and network forensics. During his career, Paul has been engaged to provide digital forensics assistance on more than 200 search warrants and criminal investigations.

Paul has significant experience in the provision of expert reports and expert testimony for court proceedings on a wide range of topics.

+61 3 9908 8968 | paul.harrison@kordamentha.com

KordaMentha

Contact us

Auckland
+64 9976 4747

Brisbane
+61 7 3338 0222

Canberra
+61 2 6188 9222

Jakarta
+62 21 3972 7000

Melbourne
+61 3 8623 3333

Perth
+61 8 9220 9333

Singapore
+65 6593 9333

Sydney
+61 2 8257 3000

Townsville
+61 7 4724 9888

For more information visit
kordamentha.com

Liability limited by a scheme approved
under Professional Standards Legislation.