CAPABILITY STATEMENT

DIGITAL FORENSICS AND INCIDENT RESPONSE

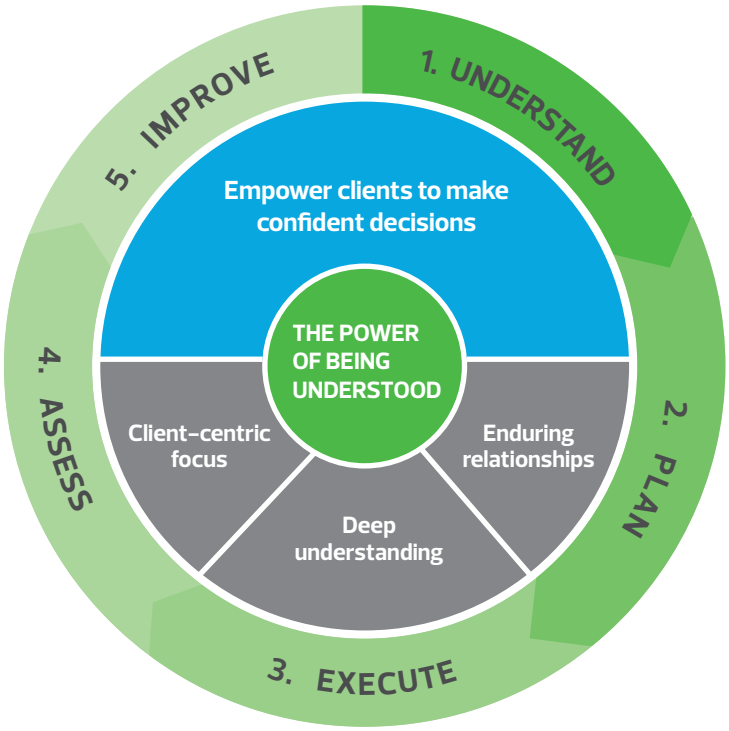
Introduction

Computer and network security has become an important part of an organisation's management control structure.

Since most organisations rely on computer systems and related application software to manage and maintain their business information, it is critical that these organisations can ensure the confidentiality, integrity and availability of their data, especially in the insurance industry.

When a security incident occurs, an efficient, prompt response is critical to maintaining business operations and minimising the financial impact and reputational damage.

RSM Australia (RSM) brings a comprehensive team with specialists that can address the needs of our clients. Our consultants' expertise centre around assisting clients with time-sensitive incident responses and helping to identify root causes to resolve incidents as expeditiously as possible. The following provides an over of RSM's service offerings and capabilities.



DIGITAL FORENSICS AND INCIDENT RESPONSE QUALIFICATIONS

The types of incidents we typically encounter fall into a range of categories, including:

- Malware
- Ransomware
- Theft of intellectual property/trade secrets
- Lost or stolen devices
- Compromised web-based email and file storage accounts

The size of the incidents ranges from a single compromised email account to thousands of systems compromised with a very aggressive malware. Typically, our incident response matters run from a few to several hundred compromised systems.

> When a security incident occurs, an efficient, prompt response is critical to maintaining business operations and minimising the financial impact and reputational damage.

RSM

Michael Shatter, is the National Director, Security and Privacy Risk Services. He is assisted by Jenny Johanson, Senior Advisor, who will oversee the daily operations of individual engagements. Ryan Easte, specialist security consultant, leads the incident response team. Other professionals at the necessary skill and experience level may be called upon to assist in the project as appropriate.

The Risk Advisory Services (RAS) group is a pillar of our consulting practice and brings a multidisciplinary approach to assessing controls across your business enterprise, with the Security & Privacy Risk Services group providing cybersecurity assessment services to clients in a variety of organisational sizes and structures. Our professionals carry a multitude of industry-recognised certifications, and Michael is a recognised thought leader within the security industry.

RSM serves clients in a wide variety of sectors, including the following:

- Financial services
- Real estate
- Business and professional services
- Consumer and industrial products
- Nonprofit organisations
- Financial institutions
- Federal, state and local government
- Education
- Insurance
- Heath care

Our core cyber incident response staff are in Melbourne. We also have other technology and security personnel who participate in cyber incident response matters located in Sydney and Perth. Michael regularly writes articles and presents on the latest issues and trends affecting your business.

The Security & Privacy Risk practice is the primary line of business for cyber offerings. Within this group we have teams that perform:

- DFIR engagements, including incident/breach response, digital forensics and investigations, eDiscovery, etc
- Security testing engagements, including ethical hacking for networks, operating systems, Enterprise Resource Planning (ERP) systems, web applications, wireless, social engineering, etc
- Security architecture engagements, including security information and event management (SIEM), data loss prevention (DLP), network monitoring, etc
- Security governance engagements

RSM has security, privacy, and risk services personnel in several locations globally. Given the developing data privacy landscape, conducting cyber incident response investigations can pose several challenges. Depending on the jurisdiction and the specific client needs, we would develop a strategy to perform the requested analysis that will address any data privacy issues. The primary focus of this international coordination is to avoid violating any of relevant privacy laws in effected jurisdictions.

RSM does offer clients an Incident Response Service Plan where a master services agreement (MSA) is established with preferred agreed-upon rates. Any required data privacy agreements (nondisclosure agreement (NDA), business associate agreement (BAA), etc.) will be completed by the parties at the time the MSA and statement of work (SOW) are issued.

For more information please contact:

Michael Shatter, Director
Security and Privacy Risk Services
T 03 9286 8166
E michael.shatter@rsm.com.au

RSM