Sense of Security

Compliance, Protection and Business Confidence

The ICT security landscape is ever-changing. As cyber threats — and cyber criminals — grow ever-more sophisticated, the security of your business becomes, at the same time, both more crucial and harder to protect. Expert security advice and solutions are no longer the province only of the largest enterprises; today, protecting your business and your IP is a vital part of overall good governance for every company.

Sense of Security®

Information Security You Can Count On

At Sense of Security, Information Security and Risk Management is our only business. Our consultants are experts in their fields; our specialists are always ahead of the curve. And so are our clients, because in security, if you are not ahead of the curve, you are at risk of becoming the next victim. By engaging Sense of Security, our clients ensure they are protected, their information is safe from threats from both within and outside the organisation, they meet their regulatory requirements and their employees, partners and suppliers can conduct business in complete confidence.

Our Experience

Founded in 2002, Sense of Security began as a partnership between two security professionals who delight in investigating the depths of information defence. The company now has offices in Sydney and Melbourne, with a consulting resource pool who travel nationally and regionally wherever our clients require them. Mitigating business risks takes us from the deepest mines to the biggest boardrooms, with clients in national and multi-national enterprises as well as many public sector organisations.

Technically outstanding and exceptionally detail oriented, from the very beginning our focus has been on conducting our business to the highest possible standards. To further this aim, we have established a research laboratory where we conduct detailed analysis of security vulnerabilities. As a result of this expertise, we are often asked to present to industry associations and conferences. We also run a series of webinars on topics of interest for our clients and the broader information security community.

Having gained a reputation for high quality work, our excellence has been recognised by the marketplace through national and international awards from respected entities such as BRW and Deloitte for being one of Australia's fastest growing, most superior technological enterprises.

Our culture is based on integrity, ethics, quality, independence and value. We view our accountability to our clients and to the wider community extremely seriously. We do our utmost to conduct our business in a sustainable manner. As industry thought leaders, we undertake a variety of social responsibility activities to educate society on how to avoid and address information security issues.

Our Clients

Highly regulated industries are a natural fit for Sense of Security — our services are used by many major names in the Banking and Finance, Insurance, Healthcare and Retail sectors as well as Resources, Utilities and Telecommunications. In the public arena we conduct business with Local, State, and Federal governments. We have been selected on numerous government panels which not only enable us to undertake extensive work for government but also demonstrate our capacity and credibility to the broader market place.

Extensive recognition in the form of awards attests to our credentials. Whilst we also have clients who are happy to provide verbal references to prospective customers, because our business is security, we choose to protect both our own IP and our clients' with contractual mutual confidentiality conditions under which client details are kept out of the public domain.

Industry Trends

Today's businesses are supported by technology ecosystems that continue to evolve at a break neck speed. Online applications, 'big data', consumerism, mobile devices, and cloud computing are some of the paradigms shaping the way organisations use information to interact with their people, customers, and wider stakeholders.

To add to the complexity, organisations and IT executives are confronted with a workforce that places a high value on use of privately owned smart phones and tablets (the BYOD phenomenon) for business and personal purposes.

These trends are occurring in a global environment where the threat landscape to all organisations and sectors has markedly intensified. Incidents of cyber-attack, cyber espionage, ransomware, insider threat and Hacktivism are reported by the media frequently. Australia is not immune to this trend with many security breaches cited over the past 12 month period alone. Many of these incidents were the direct result of a weakness (vulnerability) in technology, people or a process.

Accordingly, a greater emphasis on robust information security strategy, policy, management practices, and reporting is required for the custodians of our information assets. In Australia we have recognised this responsibility in a number of forms including most recently through the Privacy Amendment Act. This Act includes a set of new, harmonised, privacy principles that will regulate the handling of personal information by both Australian government agencies and businesses. These new principles are called the Australian Privacy Principles (APPs).

Executive level participation and responsibility is self-evident, a renewed focus on the obligations of directors under aspects of the Corporations Act is expected for many.

> "In an increasingly hyperconnected world, the impacts of our successes and mistakes are significantly magnified. Resilience of cyberspace could be strengthened by treating cyber security as a board-level issue…"
> — The World Risk Report, 2013 — The World Economic Forum

Our Research

Through the technical assessments Sense of Security undertakes, we regularly become aware of flaws in common commercial and open technology platforms. We have invested in a research laboratory where we conduct detailed analysis on identified vulnerabilities and then advise the vendor(s) if there is a previously unknown issue that needs to be addressed. When the vendor(s) have made a fix available we notify our clients. Furthermore we publish the results of our research free of charge on our corporate website (www.senseofsecurity.com.au) for the benefit of the community at large.

Developing the Sense of Security knowledge bank further, we conduct quarterly webinars on popular topics (such as the security issues presented by virtualisation and Smartphone security) as a complimentary service for our clients and prospective clients.

In the same spirit, we regularly present to interest groups, associations and conferences. We are the most active consultancy in Australia in delivering security advisories, education and awareness to the community in relation to the risks and implications of online activity. We are not paid for the effort involved, instead viewing it as part of our contribution to improving security awareness and raising the global standard of information security.

Our Services

Organisations are generally at more risk than they think they are, believing that what they don't know doesn't hurt them. On the contrary, due to the sophistication of today's attack many businesses succumb to external and internal attacks. Where there is no detection process, companies are often not even conscious that they are compromised ... and then it's too late.

Rather than relying on ad hoc technical testing only, Sense of Security clients move through a top-down process, implementing a management framework to assist them with information security and risk. It's an approach that is industry-aligned and practical for any organisation, emphasising greater protection on key assets and a business need-to-know policy. This structured approach delivers confidence that the organisation has the right framework in place whilst also enhancing a company's reputation to clients.

Building security controls into a business starts with a risk assessment to understand where key information assets are and drive management practices to ensure that those critical assets are secured. Results of the risk assessment may indicate that elements of a company's architecture need to be assessed or redesigned. Furthermore additional security controls may be needed or detailed security testing of certain assets might be required to ensure their security and compliance with best-practice standards.

In this increasingly compliance-conscious world, most organisations now recognise the need to move from ad hoc security and risk management controls to a best-practice information security management system (ISMS). The most widely recognised ISMS is the International Organisation for Standardisation (ISO) 27000-series standards. Adopting ISO 27001 reduces business risks by requiring an organisation to be formally audited and certified as compliant with the standard, then continuing to undergo regular assessments to make certain that information security controls and thus, acceptable levels of risk, are maintained.

Sense of Security provides an extensive Governance, Risk and Compliance consulting capability, ensuring that our clients are able to meet all appropriate standards. Our ISO 27001 lead auditors advise, assess, implement and qualify our clients' standards and governance regulatory requirements.

Similarly, for the Payment Card Industry, we are a Qualified Security Assessor (QSA) company endorsed by the PCI Security Standards Council. Organisations that process, transmit and store credit card data are obliged to comply with the Payment Card Industry Data Security Standard (PCI DSS). We assist organisations who need to comply with this global standard to meet their compliance objectives.

GOVERNANCE, RISK & COMPLIANCE

- ISMS Development – ISO 27001/2
- Risk Management
- PCI Data Security Standard
- Privacy Act & Personal Information Security
- Australian Government Security Standards (ISM, PSPF & NESAF)
- Cloud Computing Security Governance
- Third Party Governance & Management
- Secure Development Lifecycle

SECURITY STRATEGY & ARCHITECTURE

- Information Security Architecture & Strategy
- Information Security Policy & Procedure Development
- Cyber Threat & Risk Assesment/Treatment
- Vulnerability Management
- Cloud Security Architecture
- Information Security Training
- SCADA Secure Design & Review

TECHNICAL ASSESSMENT & ASSURANCE

- Penetration Testing
- Host & Device Security
- Application Security
- Mobile Solution Security
- Human Factor Security (Social Engineering)
- Red Team Exercise
- ERP Security
- Unified Communications Security
- IoT Security

"Cyberspace is a 24 hour a day world, one in which old assumptions about geographic boundaries and time zones are obsolete. This is one of the great benefits of modern technology — cyberspace is always open for business. But this also brings great challenges to those who guard our electronic borders."

Senator John Faulkner

Choose Sense of Security

Our Accreditation

Credentials are the benchmarks we live by at Sense of Security; they're a vital part of our organisation. We have worked hard to reach our current high standards. Our firm and consultants are proud to be associated with numerous professional bodies including memberships of the following:

- Council for Registered Ethical Security Testers (CREST) Approved Company
- Australian Information Security Association (AISA)
- Information Systems Audit and Control Association (ISACA)
- National Computer Emergency Response Team for Australia and a leading CERT in the Asia/Pacific region (AusCERT)
- Australian Institute of Company Directors
- NSW Government - Security Licensing & Enforcement Directorate (SLED)

Choose Sense of Security

Choose Sense of Security for our expertise and our experience. Choose us for the quality of our work, our broad product knowledge and intellectual property, our superior and diverse skills, our resource availability, our certifications and our effective deliverables. Choose us because we are Australia's premier independent security and risk management solution provider. Choose us because of our industry-leading awards. Choose us for our specialised industry knowledge.

Choose us because our solutions deliver on their promises so that your business can continue to deliver on yours.

Our consultants hold a broad range of industry certifications of which the following are a sample:

GOVERNANCE, RISK & COMPLIANCE

ISO 27001 Lead Auditor

Australian Signals Directorate – Information Security Registered Assessors Program

Payment Card Industry Qualified Security Assessor (PCI QSA)

Certified in Risk and Information Systems Control (CRISC)

Certified Information Systems Auditor (CISA)

Certified Information Security Manager (CISM)

Certified Information Systems Security Professional (CISSP)

ITIL v.3 Foundation Certificate

TECHNICAL ASSESSMENT & ASSURANCE

CREST Certified Web Application Tester

CREST Certified Tester

Certified Secure Software Lifecycle Professional

Certified Information Systems Security Professional (CISSP)

GIAC Certified Intrusion Analyst (SANS)

Offensive Security Certified Professional

Offensive Security Wireless Professional

Certified Penetration Testing Professional

SANS Reverse Engineering Malware

Sense of Security®

For More Information

To discuss how our security solutions can help protect your most vital assets, please call us on **1300 922 923** or **+61 (2) 9290 4444.**

SYDNEY Level 8, 66 King St, Sydney, NSW 2000

MELBOURNE Level 15, 401 Docklands Dr, Docklands, VIC 3008

info@senseofsecurity.com.au
www.senseofsecurity.com.au