Certified B Corporation

Phronesis Security

Service Catalogue

World-class cyber security consulting with a tangible social and environmental impact

Service Offerings

At Phronesis Security, we pride ourselves on delivering services that make cyber security a business enabler, not an obstacle.

We understand that most cyber problems have multiple possible solutions and our clients trust us to help them make risk-informed decisions that maximise return on security investment.

Our services can help you understand cyber risk, meet compliance and strategy objectives, select and continuously improve fit-for-purpose security controls, identify and protect information assets, and anticipate and effectively manage cyber incidents.

This document details our key service offerings including benefits and outcomes, success stories, and examples of our most commonly utilised services.

1. Governance, Risk & Compliance
2. Penetration Testing
3. Security Architecture
4. Security Awareness
5. Strategy & Management

Governance, Risk & Compliance

Cost-effective solutions for mitigating risks and achieving compliance goals

Clearer, More Actionable

security programs supported by the definition, documentation, and communication of effective governance structures and responsibilities

Increased Return on Investment

from the cyber security budget by defining and prioritising control selection and implementation through pragmatic cyber security risk assessment

Picking the Right Tool for the Job

by understanding your organisation's underlying business drivers and external dependencies when selecting security frameworks and addressing compliance objectives

Governance, Risk and Compliance (GRC) is about ensuring your organisation is hitting its cyber security targets as defined in law, regulation or policy, with clear accountabilities and pragmatic management of risk.

Our GRC Leadership team have over 70 years' combined experience in delivering programs of this kind, to clients of every kind. Our most common engagements are as follows:

- Threat and Risk Assessments
- ISO 27001 Compliance Programs
- NIST CSF Maturity Assessments
- IRAP and ISM Assessments
- SOC 2 reporting
- PCI-DSS Assessments
- State goverment attestations, such as NSW Mandatory Requirements, VPDSS, IS18

Penetration Testing

Verify how well applications, websites, networks, and devices are really protected

Manage Vulnerabilities

including how to anticipate and identify their emergence, methods and viability of exploitation, and selecting and implementing effective security controls

Gain Real Insight

into the potential impact of an attack, to better judge the risk of vulnerabilities in buildings, systems, applications or devices

Clear, Practicable Advice

on how to remediate identified issues with advice from our expert consultants with real-world experience in fixing the same issues for similar organisations

Penetration testing is the practice of simulating a cyberattack by an expert to identify vulnerabilities and test defences. Using the same tools, tactics and techniques as an adversary, we verify the efficacy of controls, attempt to exploit identified vulnerabilities, and communicate the potential business impacts to the organisation.

- Internal Penetration Testing replicates an attacker with access to your internal systems or network - either a malicious insider or a threat that has already established access.
- External Penetration Testing is conducted remotely and replicates an Internet-based attacker attempting to gain access to your systems or network.
- Cloud Penetration Testing simulates an attacker targeting your cloud environment, such as Amazon AWS, Microsoft Azure or Google GCP.
- Web Application Penetration Testing tests a web application, web service or API, replicating an attack based on a threat with various levels of access to your web application.
- IOT Penetration Testing is the identification, assessment and exploitation of various components present in an Internet of Things (IoT) device solution.

Security Architecture

Get the most out of your security people, processes and technologies

Increased Return on Investment

by analysing business goals and objectives, and converting these into security architecture principles and requirements

Provides Visibility and Insight

to cyber security risks resulting from service and technology usage by creating traceability between security and business requirements

Reduced Project Costs

by identifying and planning cyber security requirements into the early stages of projects, rather than attempting to 'bolt on' controls after the project is delivered

Security architecture is composed of the principles, methods, tools, and frameworks that protect an organisation's assets from threats. Security architecture can be applied to an entire organisation or to individual applications, processes, networks, cloud environments, or infrastructure.

- Enterprise Security Architecture involves developing strategy for the secure implementation and management of technology across an entire organisation to align with business goals and strategies.
- Security Solutions Architecture provides technical security assistance to security or non security-focused projects. This includes developing business cases, crafting tailored strategies (such as an Identity and Access Management Strategy or Cloud Security Strategy), or providing technical leadership and advisory.
- Security Architecture Assessment identifies and prioritises risks and risk treatments for a specific target system (application, cloud, network, or infrastructure), including its supporting people, processes, and technologies.
- Configuration Assessment is a review of the implementation and configuration of an asset (such as a cloud environment or network device) against security industry standards and vendor best practices to identify cost-effective opportunities for improvement.

Security Awareness

Highly modular and impactful campaigns to empower and educate your workforce

Reduce Cyber Security Risk

by providing tailored training and education to general or specific user groups based on policy, internal processes, and business risk exposure

Increase Incident Reporting

by boosting awareness, reducing the time between detection and response, and improving your organisation's cyber security culture

Reputational Assurance

through knowing your information is being stored and processed by staff and third parties who understand their security responsibilities and your organisation's information handling requirements

Cyber security awareness and education can turn your people from the organisation's greatest vulnerability to its first line of defence.

The world's leading data breach report – the Verizon Data Breach Investigations Report – indicates that 82% of breaches involve the human element. That is why Security Awareness and Education (SAE) has never been more important. Our most utilised SAE services are:

- Education strategies, for tracking and improving awareness and engagement via tailored combinations of the services below.
- Security awareness baselining, through formative assessment techniques benchmarked against the NIST NICE Framework.
- Security awareness training, for all staff, personnel with elevated privileges or risk, third parties, executives, travel and device security, as well as regular 'refresher' sessions.
- Creative content development, such as blogs, posters, comics, videos, or choose-your own-adventure courses to provide high-impact, low effort reinforcement of key security concepts.
- Validation exercises, such as phishing simulation tests, user surveys and threat modelling workshops
- Designing and facilitating Tailored Crisis or Breach Response Simulations to stress test an organisations people and process and identify shortcomings in a safe and controlled manner.

Strategy & Management

Virtual CISO, pragmatic security strategies and programs, and advisory on-demand

Burst Capacity

to access to a broad range of skills and services within a single engagement, for when you need it most

World-class Expertise

leveraging industry leaders with experience driving cyber transformation programs for some of the world's most recognisable organisations via our proven virtual Chief Information Security Officer (vCISO) offering

Wholistic Approaches

tailored to your organisation's unique operating environment and threat context, so your cyber security function is fit-for-purpose and integrates with the rest of the business.

Effective security management begins at the top and is driven by a proactive, risk-informed culture. Our Strategy and Management service, either led by a vCISO or utilising on-demand advisory services, can be tailored to any organisation's requirements, large or small.

Our focus is maximising performance improvement while optimising return on investment from your cyber security budget. Our most utilised Strategy and Management engagement are:

- Security management and reporting, including program/project management, resourcing support, recruitment vetting, and performance metrics reporting to the board and C-Suite.
- On-demand advisory and technical implementation support to deliver cyber security projects or strategy initiatives, so you have access to the right people for the right problems at the right time.
- Organisation-wide threat modelling and risk management, to ensure the full spectrum of threats and risks are identified and managed across your organisation.
- Security strategy definition and delivery, to ensure your organisation is achieving its cyber security objectives.
- Security maturity roadmapping, benchmarked against the NIST-CSF to provide clarity of vision and cost-effective control selection.
- Budget analysis and planning, including Annualized Loss Expectancy and Mitigation Ratio assessment

About Phronesis Security

Phronesis Security is Australia's first B Corp certified cyber security company, committed to delivering world-class cyber security consulting with a tangible social and environmental impact.

We recognise technology is only as effective as its configuration, and policies are just paper without proper implementation and an educated workforce. We also understand that this year's wastage could mean next year's breach.

By putting impact at the forefront of our operations, we want to demonstrate how corporate Australia can take an active role in making Australia's future cleaner, fairer and more sustainable.

To maximise our social and environmental impact, we use evidence-based metrics to identify charities that provide some of the greatest benefit per-dollar and have pledged to donate 10% of our profits accordingly.

To see the current results of our impact mission, scan the code below:

LEADERSHIP TEAM

Elliot Dellys
Chief Realist (CEO)

Daniel Hood
Chief Optimist (CTO)

Barry Grek
Director of Victoria

Eric Pinkerton
Director of NSW

Social and Environmental Responsibility

Our philosophy is grounded on the principles of effective altruism and the 80,000 hours project.

Learn more at
phronesissecurity.com/our-mission

AGAINST MALARIA FOUNDATION

Malaria kills about 400,000 people every year and more than 200 million fall ill. Bed-nets are a proven intervention - a more effective a way of saving lives than any other

AUSTRALIAN INDIGENOUS EDUCATION FOUNDATION

AIEF empowers young indigenous people to build a brighter future for themselves and the nation by providing scholarships for indigenous students in financial need

CARBON POSITIVE AUSTRALIA

To combat climate change, Carbon Positive Australia take degraded, unused land and restore the natural habitat by planting a mix of native trees and shrubs that are indigenous to the area.

Tried & Trusted

Award winning,
world-class quality services

TECHNOLOGY SCALE-UP AWARDS
2023 WINNER
Business and Professional Services of the Year
AUSTRALIAN CYBER SECURITY AWARDS 2023
FINALIST
Cyber Security Consulting Company of the Year
2021
AUSTRALIAN WOMEN IN SECURITY AWARDS
MALE CHAMPION OF CHANGE
NOMINEE
AISA AWARDS
FINALIST
CYBER SECURITY SMB OF THE YEAR
2023

Awards

- Winner of ‘Professional Services Company of the Year’ in the Technology Scale-Up Awards (2023)
- Finalist for ‘Cyber Security Consulting Company of the Year’ in the Australian Cyber Security Awards (2023)
- Finalist for ‘SMB of the Year’ in the Australian Information Security Association (AISA) Awards (2023)
- Finalist for ‘Rising Star Award’ in the Australian Information Security Association (AISA) Awards (2023)
- Nominated for the ‘Champion of Change Award’ by the Australian Women in Security Network (AWSN) (2021)

Testimonials

The team at Phronesis always deliver a quality outcome with the expertise and thought leadership up to the task.

D. Mathieson
Chief Information Security Officer
NSW Government

Phronesis have been an absolute pleasure to work with in every respect. Phronesis have a great team with a range of skills both technical and non-technical to meet our requirements.

D. Hammond
Chief Information Security Officer
Social Services Provider

As always, you guys get the job done with minimal fuss. It’s been great to work with you.

A. Peter
Head of Cyber Security
Strategic Analytics Firm

> “An Integral, Reliable,
> Efficient Partner”

Certifications

CISA
CRISC
CISM
CISSP
CREST
PCI
irap
LEAD AUDITOR
ISO 27001
aws certified
Security
Specialty

Case Studies

Critical Infrastructure vCISO

In 2021, Phronesis Security was appointed the virtual Chief Information Security Officer (vCISO) for an Australian critical infrastructure provider with $2.2 billion in assets and an annual turnover of approximately AUD$400 million.

This engagement involved amending and driving the client's three-year cyber security strategy, with a mandate covering all aspects of information security including but not limited to compliance, people, education and culture, digital asset protection, and incident response.

Key achievements within this engagement include:

- Building a cyber security team from the ground up to support ongoing compliance and operations
- The development and implementation of a sophisticated cyber security risk management framework covering ICT and OT infrastructure
- The delivery of a compliance program to ensure ongoing alignment to the Security Legislation Amendment (Critical Infrastructure Protection) Act 2022
- The development of a suite of ISO27001:2013 compliant cyber security policies and procedures

NSW Government Incident Response Uplift

Between 2021-2022, Phronesis Security was engaged to design and deliver an incident response uplift program for sixteen (16) different NSW Government agencies.

Phronesis Security's objective was to provide a unified and consistent method of identifying, managing, and reporting cyber incidents across the state. This involved the development and testing of incident response plans (IRPs), communications plans, incident tracking procedures, and incident response 'playbooks'.

Agencies within the scope of this program included law enforcement, cultural institutions, and service delivery entities, with a diverse range of ICT environments, security maturity, and legal and regulatory drivers.

Each agency was benchmarked against the NIST-CSF at commencement and completion of the engagement to enable continuous improvement and monitoring of cyber security maturity. The result was a tangible and measurable improvement in incident response maturity, in addition to providing a mechanism for enabling more cost-effective cyber security expenditure across the state.

This engagement was delivered within scope, budget and schedule, despite occurring over holiday periods and COVID-19 lockdowns. All client stakeholders commended Phronesis Security for the targeted and impactful delivery of crucial incident response capabilities, with the company since becoming a trusted partner and providing ongoing across the NSW Government cluster.

Case Studies

Vulnerability Management Program

In 2023, Phronesis Security assisted a major Australian payment processing provider in the identification of 5000 technical vulnerabilities rated as either critical or high risk – a significant challenge for any business.

To assist, Phronesis Security developed a tailored strategy that automated the categorisation of vulnerable devices according to business purpose and technical risk, reflective of cutting-edge vulnerability management best practices ("contextual CVSS scoring", as per Gartner's "Asset Context Prioritisation" or Cisco's "Business Risk Observability" metrics).

To enable root cause analysis and prevent recurrence, Phronesis Security subsequently developed custom dashboards to provide alerting based on both asset value and vulnerability criticality, ensuring the client's response teams could quickly and accurately remediate emerging issues.

As a result, Phronesis Security has been engaged to provide weekly updates to the CIO and CEO, who now have far greater technical and business insight into their organisation's cyber risk posture.

Cyber Security Awareness and Education Program

Since early 2022, Phronesis Security has been engaged by a leading health and community services non-profit in a wide range of cyber security uplift activities. The first was to consult with all relevant internal and external business stakeholders to design a pragmatic and fit-for-purpose information security management system (ISMS).

The outcome was a suite of documentation tailored to the organisation's operating and threat context, including an Information Security Risk Management Framework, an Incident Response Plan and 18 domain-specific standards covering topics such as cryptography and identity and access management.

Phronesis Security has subsequently become a long-term security partner, providing penetration testing, security awareness, information asset management, security operations support, and vendor risk management services.

This engagement has been a testament to the high level of trust placed in Phronesis Security, which we pride ourselves on maintaining with all our clients.

For further case studies, testimonials and references, get in touch at info@phronesissecurity.com

Phronesis Security

To learn more, get in touch today

☎ 1300 PHRONESIS

🌐 www.phronesissecurity.com

✉ info@phronesissecurity.com