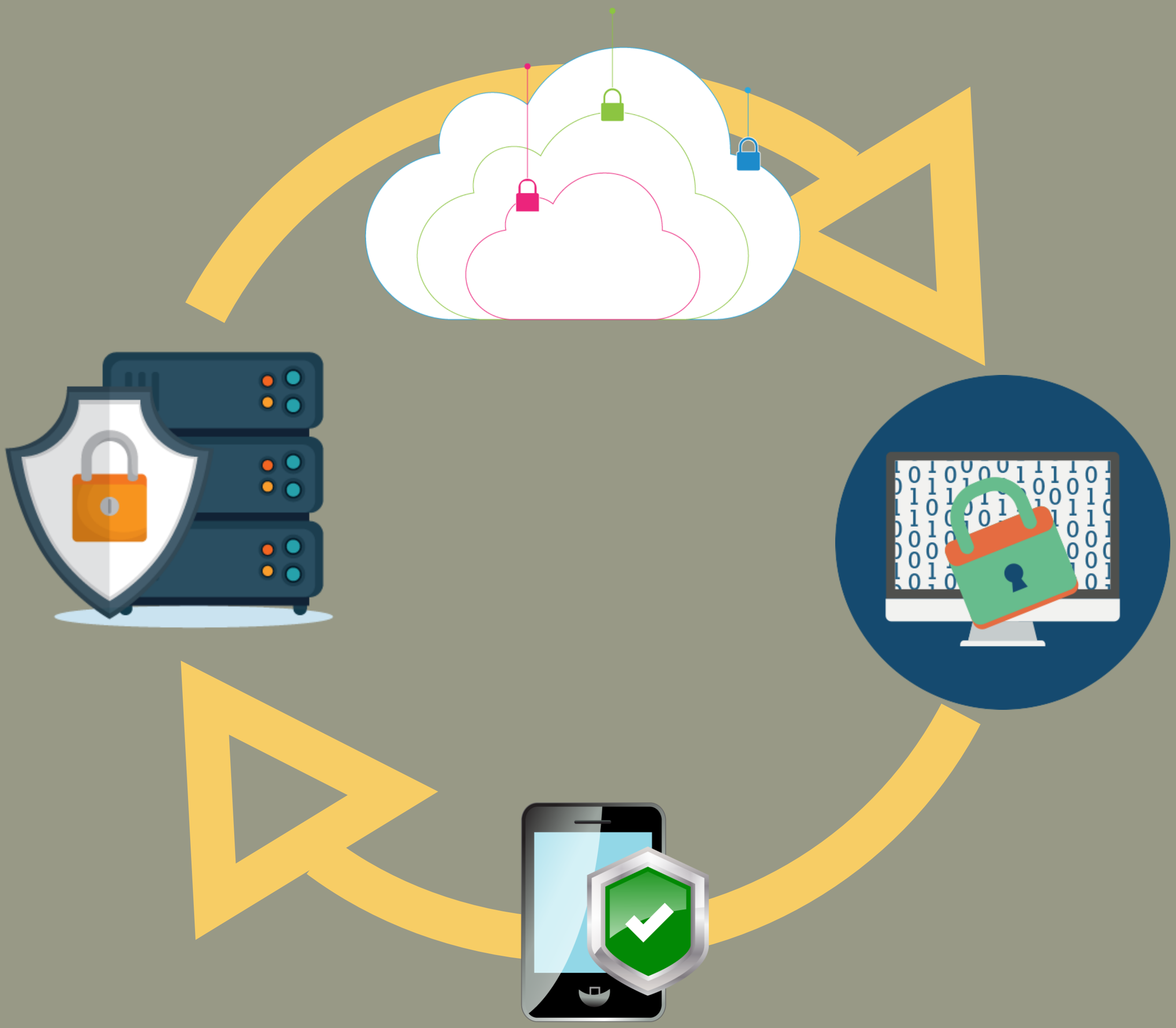
RECOGNITE

OBSERVATION CONSULTANCY SOLUTION

IT SECURITY SERVICES

www.recognite.com.au

Level 2/570 St Kilda
Road, Melbourne



Security Audit

Penetration Testing

Social Engineering

Security As A Service

Breach Remediation

OUR CAPABILITIES:

- Penetration testing
- Investigating social engineering vulnerabilities
- Application testing
- Red teaming
- Provide training on social hacking as well as IT and data security
- Non-functional testing of IT and data security
- PCI DSS compliance
- Providing remediation
- Training on IT and data security
- Conducting IT and data security and architecture reviews
- Providing reports to management on IT security plus recommended processes and procedures
- Providing reports to management on areas of vulnerability
- Providing services for the full outsourcing of IT and data security

ReCognite lead the way in providing effective IT security solutions to mitigate risk for your business. We ensure the security audit and implementation is seamless and disruption to your business is minimised.

HOW SAFE IS YOUR DATA?

Businesses and organisations face the ongoing challenge: how safe is my data and information? The rapid pace at which the cyber security landscape changes is proving a challenge for many businesses.

With our extensive IT cyber security knowledge, ReCognite and our expert network provides IT and data security assurance to over 1,600 clients. Our highly experienced specialists will work collaboratively with your business to gain a detailed understanding of the industry and the environment in which you operate.

ReCognite specialise in audit and penetration testing, IDR and managed IT services. We are leaders in social engineering prevention with Australian-based specialist engineers. Our testing models are designed around real-world attack scenarios. In combination with our technical security testing, our social engineering services have never failed in compromising a target.

We have a history of working closely with clients in government and corporate fields covering industries such as retail, finance as well as various government departments - providing tailored IT solutions integrated with their business needs.

We also provide technical support to your staff throughout the process to ensure the security audit and implementation is seamless. Our aim is to ensure that any disruption to your business is minimised.

TYPES OF ATTACK

The Information Gatherer

This can be as simple as questioning who a firm uses for their IT support or IT security. A seemingly harmless piece of information provided as a recommendation to another person or organisation, this information can be used to phone multiple individuals masquerading as a representative of the IT company to request sensitive information ranging from remote access to passwords.

The Panic Assist

By manipulating people's willingness to help others in distress, this type of hacker provides a compelling story or scenario to gain access. For example, a person may approach reception advising them that they have a job interview and didn't print out their resume. They then ask the receptionist to help them out and print their resume from a USB key, which in turn has allowed the hacker to gain full network access.

Physical Access

Most would be surprised to know how easy it is to walk into many organisations and either connect devices to get access or simply sit down at a terminal. Our tests have proven how easy it is to unplug machines with sensitive data and walk out the front door.

Entry level and low level staff

In some businesses there is a high staff turnover in entry level and low level positions. This includes cleaners, data entry, admin and even helpdesk or customer service roles. This type of hacker secures a job in your business and it may give them access to highly sensitive data.

Phone Ahead/Phone Attack

A simple phone call can often yield remote access to a network long enough to laterally move inside an organisation and plant malicious code in an attack.

Phishing Emails

This type of hacker uses a simple email to target individuals. Unfortunately they play on curiosity or greed and use tactics that allow complete access to a system.

USB drops

You'd be surprised how often staff will pick up rogue USB devices and connect them to access data. Prevention can be easily addressed through implementation of technology and staff training.

PREVENTION

Prevention is paramount and social engineering tactics will give protection to your business.

Training - We will ensure that your staff are fully-trained and familiar with the risks associated with social engineering.

Drills - We will support your business to implement regular testing so there are no vulnerabilities present.

Penetration testing - We will support your business to implement penetration testing. This is a critical component and yet it is the most overlooked.

Process/procedure - We will support your staff to implement the processes and procedures that will prevent most attacks or detect them early.

RECOGNITE

SECURITY AS A SERVICE (SECAAS)

Security-as-a-Service (SECaaS) is a cloud-based IT security service provided through a pay-as-you-go subscription model.

SECaaS is easily managed via a console platform. Managed Security-as-a-Service supports your organisation by providing consistent and up-to-date security coverage, allowing full and ongoing visibility of your network.

The software analyses and provides alerts upon any unusual security related events such as data being copied offsite, malicious code, malware and other threats. SECaaS + IDR is the only fully integrated detection and investigation solution that lets you identify a situation where your system is compromised, as it occurs, allowing you to act quickly.

$

Cybercrime cost Australian Businesses over **$5.2B** last year, and it's rising

PENETRATION TESTING

A penetration test is an authorised hack in attempt to gain access to an organisation's data and information. ReCognite perform comprehensive penetration audits to identify vulnerabilities and measure your organisation's cyber security strength.

Penetration testing is essential to reduce and prevent the risk of data breach that can lead to significant financial and reputation damage to your organisation.

We provide full audit reporting and we work with you to establish a secure environment for your business.

Penetration testing can be performed in environments such as network and infrastructure, web platform and mobile through both internal and external testing.

SOCIAL ENGINEERING

Social engineering is the easiest method to obtain information and infiltrate an organisation's security infrastructure.

Hackers utilise deception and manipulation of staff to obtain access. It is widely known that social engineering, in the context of information security, provides the greatest risk to an organisation's security infrastructure.

Prevention whilst organisations can ensure their software is well-protected and up-to-date, it is their own staff who may inadvertently create the biggest risk for potential security attacks.

There are over **126,000** hacking tutorials and videos on Youtube