NEC \Orchestrating a brighter world

NEC Cyber Security

A full range of services built on specialist expertise, industry leading technologies alongside key strategic partnerships.

au.nec.com

Local capability
National capacity
Global coverage

Industry Overview

The Australian Government has defined a cyber attack as a deliberate act through cyberspace to manipulate, disrupt, deny, degrade or destroy computers or networks, or the information resident on them, with the effect of seriously compromising national security, stability or economic prosperity.

Cyber security threats have evolved dramatically over the last decade, driven by the increased adoption of cloud computing and take up of mobile devices. Customers are facing an evolving threat landscape where attack types change daily. Organisations require a range of mitigation strategies to effectively protect digital assets and meet increasing compliance obligations.

Cyber security threats have evolved dramatically over the last decade.

Cyber attacks against enterprise and government IT systems often cost millions of dollars to recover from and these costs are rising with the massive adoption among enterprise of smart technologies and connected devices that make up the Internet of Things (IoT).

Customers are facing an evolving threat landscape.

While the IT systems of critical infrastructure providers face the same level of risk from cyber attacks as other enterprises in the private and public sectors, a cyber attack on critical infrastructure can have much broader and deeper consequences for society and the economy. This puts added pressure on organisations and influences how they design, implement and maintain their cyber defences.

Accepting the fact that the threats are both constant and, in terms of the means and methods, constantly evolving, the key to successful mitigation is a proactive strategy of monitoring, detection and response. This includes close collaboration with all stakeholders in critical infrastructure operations and the involvement of senior leadership in driving and implementing strategies.

The key to successful mitigation is developing a proactive strategy of monitoring, detection and response.

A global study has found that 80% of organisations agree that over the next three years, the proliferation of connected devices, the 'Internet of Things' and 'Big Data' will make them more vulnerable to a serious cyber attack.

Threats

Threat to Government

Australian Government networks are regularly targeted by the full breadth of cyber adversaries. Attackers pose a threat to Government-held information and provision of services through both targeted and inadvertent compromises of Government networks through various techniques.

Attackers will continue to use low sophistication cyber capabilities – website defacement, the hack and release of personal or embarrassing information, Distributed Denial of Service (DDoS) activities and the hijacking of social media accounts – to generate attention and support for their cause. As such, issue-motivated groups pose only a limited threat to Government networks, with possible effects including availability issues and embarrassment. Some attackers intend to cause disruption that is more serious and may be able to exploit poor security to have a greater impact.

Threat to Private Sector

Australian industry is persistently targeted by a broad range of malicious cyber activity, risking the profitability, competitiveness and reputation of local businesses. Activity ranges from online vandalism and cybercrime through to the theft of commercially sensitive intellectual property and negotiation strategies.

The ongoing theft of intellectual property from Australian companies continues to pose significant challenges to the future competitiveness of Australia's economy. In particular, cyber espionage impedes Australia's competitive advantage in exclusive and profitable areas of research and development – including intellectual property generated within our universities, public and private research firms and Government sector – and provides this advantage to foreign competitors.

Examples of Threats

Spear Phishing

Emails containing a malicious link or file attachment. This remains a popular exploitation technique for many cyber adversaries, with methods used becoming more convincing and difficult to spot. As such, spear phishing emails continue to be a common exploitation technique used in the compromise of Australian industry networks.

Attackers are targeting industry personnel to gain access to corporate networks; individuals with a large amount of personal or corporate information online make it easier for adversaries to target that individual or their organisation. Attackers also make use of publicly available industry information such as annual reports, shareholder updates and media releases to craft their spear phishing emails, and use sophisticated malware to evade detection.

Ransomware

A type of malware that prevents or limits users from accessing their systems. Ransomware encrypts the files on a computer (including network shared files and attached external storage devices) then directs the victim to a webpage with instructions on how to pay a ransom in bitcoin to unlock the files. The ransom demanded in Australia has typically ranged from anything up to tens of thousands of dollars.

IoT and Big Data is making organisations more vulnerable to cyber attacks.

SecondaryTargeting

Cyber attackers attempting to gain access to enabling targets – targets of seemingly limited value but which share a trust relationship with a higher value target organisation. It is imperative that organisations understand that they might be targeted solely based on their connections with other organisations – the real target of these adversaries.

Keystroke Logging

The act of tracking and recording every keystroke entry made on a computer, often without the permission or knowledge of the user. Attackers deploy software or a hardware device on to target machines or networks. Each keystroke is recorded and re-routed to the attackers. Real-time alerts can be set up to enable attackers to receive instant updates on exactly what is being typed.

SQL Injection

A type of security exploit in which the attacker adds Structured Query Language (SQL) code to a web form input box to gain access to resources or make changes to data. An SQL query is a request for some action to be performed on a database. On a web form for user authentication, when a user enters their name and password into the text boxes provided for them, those values are inserted into a SELECT query. If the values entered are found as expected, the user is allowed access; if they aren't found, access is denied. However, most web forms have no mechanisms in place to block input other than names and passwords. Attackers can use the input boxes to send their own request to the database, which could allow them to download the entire database or interact with it in other illicit ways.

Bug Poaching

Refers to when an attacker breaks into a network and creates an analysis of the network's private information and vulnerabilities. The attacker will then contact the organisation with evidence of the breach and demand ransom – similar to ransomware. Unlike a typical ransomware attack, once information is stolen, an attacker will extort the company for information on how their system was breached, rather than the stolen data itself.

Distributed Denial of Service (DDoS)

An attack in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The victim's site struggles to address all traffic requests, which slows performance and eventually brings the site down. DDoS can act as a smokescreen for other threats.

Cross-Site Scripting

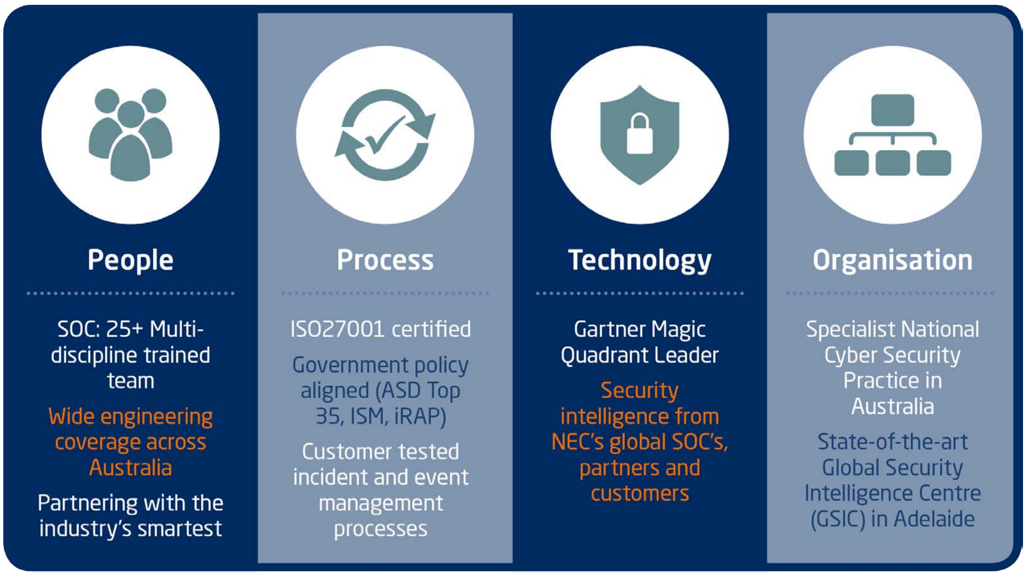
An attack which is carried out on web applications that accept input, but do not properly separate data and executable code before the input is delivered back to a user's browser. An attacker loads malicious script via a webpage, which is then saved into a database. Valid site users then enter data into this database via webpage at which time a call back is made to the attacker with the relevant data requested.

An always-on service enables businesses to improve awareness and reduce risk around the clock.

Our Approach

Responding to these challenges, NEC Australia has established a Global Security Intelligence Centre (GSIC). Complementing NEC's investment in Austria, Brazil, Japan, Singapore and the United States of America, the state-of-the-art facility develops, delivers and extends NEC Australia's cyber security capabilities - providing a rich and ever expanding suite of cyber security services.

Our cyber security framework is focussed on People, Process, Technology and Organisation to ensure that our customers effectively manage their exposure to cyber attack. We offer a broad range of security solutions and services, from consulting and integration through to managed security services and 'as a service' security services.



People

SOC: 25+ Multi-discipline trained team

Wide engineering coverage across Australia

Partnering with the industry's smartest

Process

ISO27001 certified

Government policy aligned (ASD Top 35, ISM, iRAP)

Customer tested incident and event management processes

Technology

Gartner Magic Quadrant Leader

Security intelligence from NEC's global SOC's, partners and customers

Organisation

Specialist National Cyber Security Practice in Australia

State-of-the-art Global Security Intelligence Centre (GSIC) in Adelaide

NEC's cyber security framework is focussed on people, process, technology and organisation.

Our Services

NEC Australia provides a comprehensive range of cyber security services to the private and public sectors from the GSIC in Adelaide, South Australia. This centre includes a state of the art Security Operation Centre (SOC) and industry experts providing professional services. We identify five layers, all of which are critical to a fully integrated cyber security program. Governance, risk and compliance underpin these layers.

Governance, Risk & Compliance

- Policies and Standards Development
- Policy Management
- Compliance Management
- Vendor Management
- Audit Management
- IT Risk Management
- Risk and Compliance Dashboard
- Security Awareness & Training

Threat & Vulnerability Management

- Vulnerability Management
- Penetration Testing
- Threat Management

Security Monitoring & Response

- Security Incident & Event Management (SIEM)
- Real-time Analysis
- Security Incident Management
- Threat Intelligence
- Counter Threat Management

Data Protection

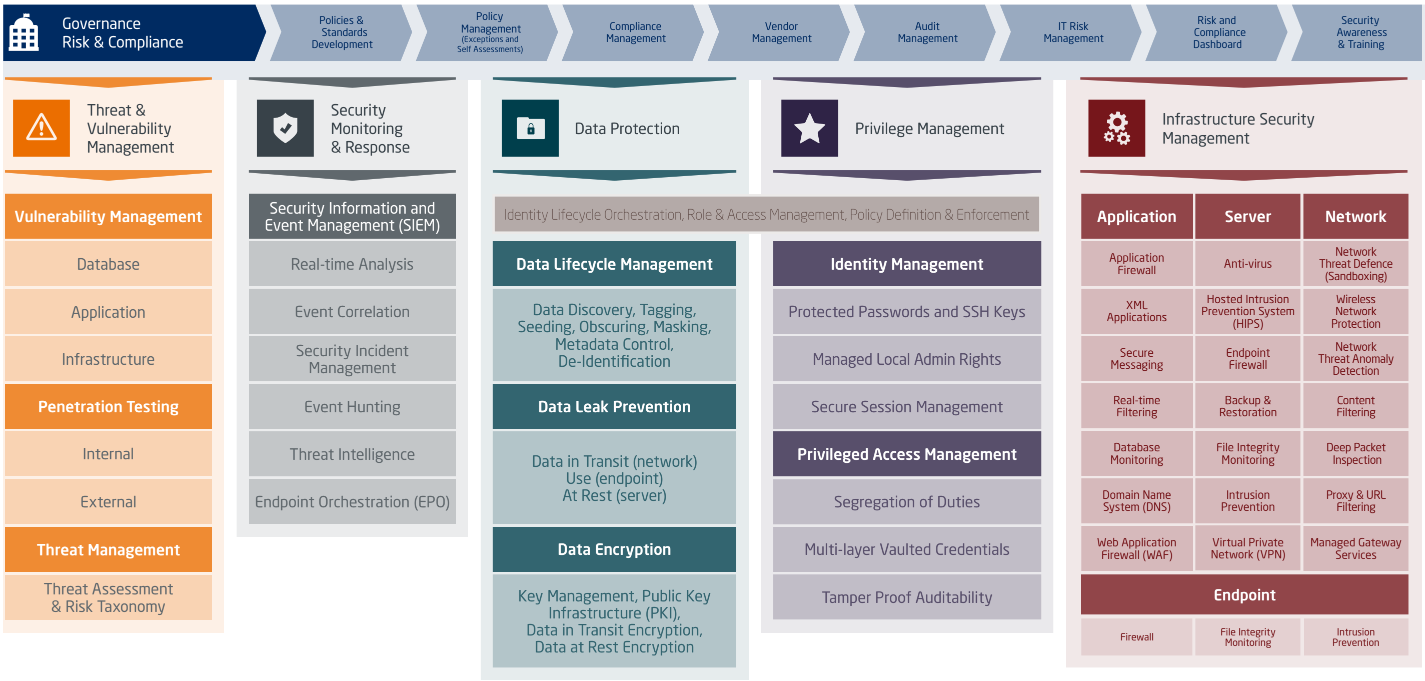
- Data Encryption
- Data Leak Protection
- Data Lifecycle Management

Privilege Management

- Identity Management
- Privileged Access Management

Infrastructure Security Management

- Application
- Endpoint
- Network
- Server



Governance Risk & Compliance

Policies & Standards Development · Policy Management (Exceptions and Self Assessments) · Compliance Management · Vendor Management · Audit Management · IT Risk Management · Risk and Compliance Dashboard · Security Awareness & Training

Threat & Vulnerability Management

- **Vulnerability Management**
  - Database
  - Application
  - Infrastructure
- **Penetration Testing**
  - Internal
  - External
- **Threat Management**
  - Threat Assessment & Risk Taxonomy

Security Monitoring & Response

- **Security Information and Event Management (SIEM)**
  - Real-time Analysis
  - Event Correlation
  - Security Incident Management
  - Event Hunting
  - Threat Intelligence
  - Endpoint Orchestration (EPO)

Identity Lifecycle Orchestration, Role & Access Management, Policy Definition & Enforcement

Data Protection

- **Data Lifecycle Management**
  - Data Discovery, Tagging, Seeding, Obscuring, Masking, Metadata Control, De-Identification
- **Data Leak Prevention**
  - Data in Transit (network)
Use (endpoint)
At Rest (server)
- **Data Encryption**
  - Key Management, Public Key Infrastructure (PKI), Data in Transit Encryption, Data at Rest Encryption

Privilege Management

- **Identity Management**
  - Protected Passwords and SSH Keys
  - Managed Local Admin Rights
  - Secure Session Management
- **Privileged Access Management**
  - Segregation of Duties
  - Multi-layer Vaulted Credentials
  - Tamper Proof Auditability

Infrastructure Security Management

Application	Server	Network
Application Firewall	Anti-virus	Network Threat Defence (Sandboxing)
XML Applications	Hosted Intrusion Prevention System (HIPS)	Wireless Network Protection
Secure Messaging	Endpoint Firewall	Network Threat Anomaly Detection
Real-time Filtering	Backup & Restoration	Content Filtering
Database Monitoring	File Integrity Monitoring	Deep Packet Inspection
Domain Name System (DNS)	Intrusion Prevention	Proxy & URL Filtering
Web Application Firewall (WAF)	Virtual Private Network (VPN)	Managed Gateway Services
Endpoint		
Firewall	File Integrity Monitoring	Intrusion Prevention

NEC cyber security services - spread across IT layers.

The Risk

No organisation is immune from cyber-crime. While capital investment to build and implement a cyber security strategy may seem high, business leaders should consider the associated costs if a serious compromise occurs on their network.

In the event of a network compromise, not only will organisations be faced with the cost of implementing these strategies to prevent further compromise, they will also incur both higher direct and indirect costs associated with remediation. These include:

- Broader costs to the Australian economy where information is stolen from networks, e.g. personal information used to conduct fraud.
- Loss of revenue associated with the theft of information, such as intellectual property, or information about Australia’s negotiating position.
- Lost productivity and income, and the costs of diverting staff and resources from other business to deal with a compromise.
- Reactive implementation strategies to mitigate further intrusions – this is more expensive to do in response to an incident, as timeframes are more compressed compared to implementing these strategies proactively.
- Reputational costs, including negative social and news media exposure and the trust of your customers, for example in the case of disruption to the availability of online services.
- Resources to investigate the extent of the intrusion, understanding the harm, and the immediate remediation of the intrusion e.g. cyber security specialists.

Why partner with NEC?

Organisations are typically unable to cope with the complexity of cyber security threats and struggle to fill the knowledge and skills gaps as well as the initial investments needed to provide suitable support and technology.

Adoption of cloud services amongst the majority of organisations is also causing visibility and control issues, which actually hold back adopting new, innovative technologies due to unknown risks.

NEC has proven capability in the security space, backed by a $4.38 million investment in the new GSIC facility located in Adelaide. The centre offers a wide range of security services delivered using a state of the art SOC environment by NEC security experts.

The GSIC also connects with global NEC Security Operations Centres that include Japan, Singapore, Europe, and the Americas to offer true global coverage and sharing of threat intelligence.

Furthermore, our cyber security services can easily integrate into our broader suite of ICT solutions and managed services. Our expertise in designing, implementing, and supporting high-quality end-to-end solutions ensures the best possible security outcomes for our customers.

NEC Australia supports over 1,300 organisations across the country.

Benefits of an NEC Managed Security Service

- Adoption of newer, cutting edge technologies to drive innovation
- Alignment to compliance, governance and policy standards
- End-to-end protection - from endpoint to cloud offering improved peace of mind
- Enhanced protection of staff and customer data
- NEC Security Operations Centre team - leverage expert analysis, escalation and incident handling
- Reduced overall cost of service ownership
- Greater visibility and control of real-time threats
- Improved security posture
- Privileged threat analytics - shortens an attacker's window of opportunity, reduces potential damage, accelerates remediation and accelerates time to value
- Reduced risk profile
- Service operates 24 x 7 x 365 - the always-on service provides out of hours coverage, improving visibility and enables businesses to improve overall security awareness and reduce risk round the clock
- The right mix of local, national and global capability to deliver the entire scope of cyber security services.

NEC's Security Operations Centre (SOC), located within our new Global Security Intelligence Centre (GSIC).

For more information, visit au.nec.com, email contactus@nec.com.au or call 131 632

Corporate Headquarters (Japan)
NEC Corporation
www.nec.com

Australia
NEC Australia Pty Ltd
au.nec.com

North America (USA)
NEC Corporation of America
www.necam.com

Asia Pacific (AP)
NEC Asia Pacific
sg.nec.com

Europe (EMEA)
NEC Enterprise Solutions
www.nec-enterprise.com

v.17.6.2 | NEC Cyber Security

NEC Australia Pty Ltd reserves the right to change product specifications, functions, or features, at any time, without notice. Please refer to your local NEC representatives for further details. Although all efforts have been made to ensure that the contents are correct, NEC shall not be liable for any direct, indirect, consequential or incidental damages resulting from the use of the equipment, manual or any related materials. The information contained herein is the property of NEC Australia Pty Ltd and shall not be reproduced without prior written approval from NEC Australia Pty Ltd.