

Orchestrating a brighter world

**NEC**

NEC Cyber Security: Vulnerability Management

# Risk & Threat Assessment



# NEC's Risk & Threat Assessment will provide a clear picture of your security posture, identifying areas of strength and weakness.

## Background

Many organisations are struggling to detect and prevent cyber threats. Despite best efforts from IT security teams and sound investments in cyber security products, malicious code, malware, botnets, Trojans and other cyber threats can still enter into your organisation.

As adoption of cloud services stretches your ICT environment into partners and increases potential risks, organisations need certainty on whether Cloud services are adequately secured and are not providing hackers and cyber threats another way into your IT systems.

Executives and directors are liable and responsible for the security of corporate information and have to ensure that diligence and due care has been applied to protect their organisation's information assets.

The Economist Intelligence Unit reports that over 36% of organisations have had a serious cyber-attack sustained which has had a material impact on operations in the past 5 years.

They also indicate that financial institutions are most at risk to cyber criminals due to the potential rewards for compromising banking and finance systems. NEC's Security Partners report that over 40% of all malicious activity was targeted at the Banking and Finance industry.

NEC's Risk & Threat Assessment will provide peace of mind for organisations to determine if current security processes and infrastructure are providing appropriate protection against security threats. It will identify gaps or issues within the current environment, from policy and process through to the network and endpoint system. This provides confidence to CEOs and directors that risks have been assessed and measured with clear recommendations for remediation.



A successful breach could mean the death of a business

## Challenges

Cyber criminals continue to develop new tricks and tools to gain access to vulnerable networks and lucrative organisational data. This changing environment is known as the threat landscape and it is very challenging for IT security teams to keep up and respond.

This is often due to:

- A poor change management and patching program
- No accurate asset inventory
- Disparate use of cloud services and insecure applications
- Handling the complexity of vulnerability information
- Aging infrastructure and lack of skilled resources

### Risk

Managing security risks is now an issue that must be managed and reported at the board level. Organisations that fail to do so can be impacted through financial fraud, extortion, reputational impacts and fines from regulators - what's important remains unknown.

Directors, executives and board members are accountable for IT security risks to an organisation and need a way for these risks to be identified, explained with recommendations on how to remove or mitigate them.

### Compliance

The majority of Australian organisations are subject to some legal and regulatory compliance obligations that cover ICT security (for example the Privacy Act). In some industries such as banking and healthcare, further obligations are in place such as PCI, APRA and Sabans-Oxley regulations.

These obligations are in place to ensure business integrity and protect the public when transacting with these organisations. If an organisation operates whilst infringing these legal and regulatory obligations, Government bodies and regulators have powers to impose severe consequences on the organisations, directors and board members.

### Governance

Changes to an organisation's IT infrastructure could result in weaker protection of information assets. Without assessing the potential impacts of these changes through a governance or assessment process, there can be unintended consequences.

It is important that any current risks and threats to an organisations IT infrastructure are assessed especially where changes have occurred without stringent governance processes in place.

## Service overview

NEC's Risk & Threat Assessment will help determine how well current security processes and systems are responding to current security challenges.

Trojans and botnets can sometimes sit dormant inside organisational networks waiting to be remotely activated – NEC's Risk & Threat Assessment will help determine if there is any suspicious activity that could indicate a Trojan or botnet that poses a serious risk to your corporate data and systems.

The service will provide a clear picture of your security posture, identifying areas of weakness. NEC's report will provide clear detail on what is important for you and provide next steps for further improvement to mitigate any identified weaknesses.

During the assessment period, NEC will analyse the following key areas:

**Security and threats** – Assessment of current patch levels across infrastructure/endpoints and known application vulnerabilities, malware, botnets and risky devices on your network.

**User activity** – What are users doing that could be putting your organisation at risk? This includes: web browsing, peer to peer applications, social media and instant messaging.

**Network utilisation** – How is the network currently used? Do the security threats and your posture adversely affect the network? Do you have enough infrastructure in place to adequately monitor the available bandwidth?

**Internet gateway architecture** – Assessment of current network and security design including defence in depth and current firewall configuration.

**Security Governance** – Review to determine if current security governance and policy are appropriate and recommendations for improving.

After the analysis, NEC will provide a report with a summary of the assessment, executive summary, industry insights, recommended actions (short and medium term) and detail of the analysis around the key areas.

This report will be reviewed face to face with you help with planning and strategy.

### Benefits

- “What’s important” to you as a business becomes known – improved visibility
- Clearly identifies what systems need to be protected from which security threats
- Provides recommendations that considers a balanced solution approach across people, procedures and technology
- Comprehensive risk profile report will prioritise security threats – reducing time to evaluate impacts and changes required
- Reduces risk of not meeting legal or regulatory compliance requirements and demonstrates that the organisation has exercised a duty of care to identify and mitigate against security threats
- Quick turnaround – preliminary report results can be available within 7 business days of probe collecting data



NEC actively looks for security risk assessment recommendations that can be implemented without expending capital

## Why NEC?

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 our suite of cyber security services and supporting our security consultants that work directly with customers and their ICT infrastructure.

Vulnerability Management is part of our broad range of security solutions and services, from consulting and integration through to managed security services and ‘as a service’ security services.

NEC Australia supports over 1,300 organisations including local state and Federal Government and enterprise clients across the country. Protecting our customers from cyber threats is built into our customer service delivery framework and even for customers that do not have specific security services, NEC will advise and guide our customers on any security risks or issues that we have visibility of.





The Threat Assessment report will be reviewed face to face with you help with planning and strategy

**To learn more about the service, please contact NEC’s Cyber Security team at: [CyberSecurity@nec.com.au](mailto:CyberSecurity@nec.com.au)**

### For more information:

 [nec.com.au](http://nec.com.au)

 [contactus@nec.com.au](mailto:contactus@nec.com.au)

 131 632

**Corporate Headquarters (Japan)**  
NEC Corporation  
[www.nec.com](http://www.nec.com)

**Australia**  
NEC Australia Pty Ltd  
[www.nec.com.au](http://www.nec.com.au)

**North America (USA)**  
NEC Corporation of America  
[www.necam.com](http://www.necam.com)

**Asia Pacific (AP)**  
NEC Asia Pacific  
[www.sg.nec.com](http://www.sg.nec.com)

**Europe (EMEA)**  
NEC Enterprise Solutions  
[www.nec-enterprise.com](http://www.nec-enterprise.com)

v190627 | NEC Cyber Security: Risk & Threat Assessment

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.

©2019 NEC Australia Pty Ltd. All rights reserved. NEC and NEC logo are trademarks or registered trademarks of NEC Corporation that may be registered in Japan and other jurisdictions. All other trademarks are the property of their respective owners. All rights reserved. Printed in Australia. Note: This disclaimer also applies to all related documents previously published.

