

# **BROADLEAF CAPITAL INTERNATIONAL PTY LTD**

ABN 24 054 021 117

23 Bettowynnd Road  
Pymble  
NSW 2073  
Australia

www.Broadleaf.com.au

Tel: +61 2 9488 8477  
Mobile: +61 4 1943 3184  
Fax: + 61 2 9488 9685  
Cooper@Broadleaf.com.au

*Specialists in Strategic, Enterprise and Project Risk Management*

## **INFORMATION AND COMMUNICATIONS TECHNOLOGY: THREAT RISK ASSESSMENTS**

### **The Need for Threat Risk Assessments**

There is an emerging need for organisations to conduct Threat Risk Assessments (TRAs) on their information and communications technology (ICT) infrastructure to identify and deal with threats to their critical systems.

While conducting a risk assessment of your critical business infrastructure can be seen simply as good governance, there are many reasons why doing a TRA is a beneficial exercise in the current environment. Among the most pressing motivations for conducting a TRA are:

- Businesses' heavy reliance on ICT and their networks;
- The potential for weaknesses in complex information networks in their design or implementation;
- The opportunity for risks to be avoided if they are identified in early design and development, avoiding costly remediation after systems are set to work;
- Certification of systems or networks containing sensitive or classified information may depend on completing a TRA; and
- Good governance requiring formal attention to threats to ICT infrastructure.

### **Information and Communications Technology Threats**

Broadleaf has conducted a number of TRAs on ICT infrastructure with large organisations. Through the conduct of these assessments, we have found most risks that arise can be grouped under a number of general headings, and that they evolve from a relatively common set of threats.

While it is important to maintain an open mind and adopt an approach that will expose any new threats, we have found there to be a number of recurring threats, which include:

- The introduction of malicious code;
- Acts of terrorism;
- System hardware or software failures;
- Natural or environmental disasters;
- Attacks on the system by external networks or hackers;
- Eavesdropping on the system; and
- User-initiated issues, either through error or malicious acts.

This short list is not exhaustive. We are finding that, as ICT systems become more complex and pervasive, new threats emerge. It is important that organisations remain vigilant to new threats and understand how they may be affected.

### **Scope of Threat Risk Assessments**

The scope of a TRA is dependent on client needs. A TRA could be focused on:

- An ICT system;
- A single component of a system; or,
- A network of systems.

Typically, a TRA will encompass, among other factors:

- People involved with the systems, including users, administrators, managers and support contractors;
- Hardware, including workstations, servers, terminal equipment and mobile computing equipment;
- Networks, including LANs and WANs, communications paths, cables and fibres;
- Software, including operating systems, corporate applications and specialised applications; and
- System governance, including procedures, processes, practices and cultural elements.

### **Approach to the Threat Risk Assessment**

Broadleaf's approach for the conduct of TRAs is based on the Australia/New Zealand Standard AS/NZS 4360:2004. This provides a consistent and logical framework for risk assessments of any type, supporting the integration of TRAs with other risk assessments and providing consistency between assessments. The Standard is the basis for risk assessments in most large organisations, both Government and private sector, and conducting TRAs in accordance with the Standard allows the results to be integrated with other organisational risk assessments, using a common language and set of measures.

We maintain an extensive list of threats that can assist clients in identifying risks in the TRA and can draw on its experience to provide a comprehensive set of ICT threats as a starting point for the conduct of an analysis. We can set up threat templates that allow risks to be identified in a logical fashion, ensuring that none are overlooked. Where it is desirable to take a fresh look, instead of or as well as using templates, we can establish a structure of key elements for the assessment that ensures effective coverage of all risks.

This approach builds on our normal risk assessment methodology, paying special attention to the importance for some clients of their own in-house threat templates and security requirements. Where clients require systems certification based on a structured TRA, a structured approach of this form is essential.

The Standard allows for a risk assessment process to be tailored to suit a specific activity. In the case of a TRA, we work with our clients to match the process to their unique requirements. Typically, this involves modifying scales for consequences and likelihood, introducing client-specific evaluation criteria, and adjusting the subsequent levels of risk severity. The result is a cost-effective process that is well matched to each ICT infrastructure requirement, and can be understood by all who participate in it and use its outcomes.

Our experience shows that the most effective way to meet the challenge of identifying all relevant risks is to conduct facilitated workshops with critical client stakeholders, including project managers, system specialists, site managers, users and administrators. Where it proves difficult to gather a group of busy ICT professionals for long enough to conduct an effective workshop, we hold structured face-to-face interviews or a mixture of interviews and workshops to achieve the same outcome.

### **Threat Risk Assessment Outcomes**

There are many direct and beneficial outcomes from the conduct of a TRA. They include:

- The development of a detailed risk register of ICT threats and risks;
- Enhanced understanding of the threats among the participants in the analysis;
- Identification of areas of high risk to an ICT system or network that can be used as the basis of treatment action planning;
- A prioritised set of risk treatment actions;
- A mature framework for ongoing management of identified risks; and
- Raised awareness about ICT security and its management.

### **Capacity to Conduct a Threat Risk Assessment**

Broadleaf offers specialised capabilities that are not available in the general consultancy community. These capabilities include:

- Staff with security clearances and an understanding of security processes within major organisations (we currently carry high levels of security clearance in the Australian Government arena);
- Detailed understanding of ICT systems, how they work and their linkages to other systems and business processes; and
- Specialised knowledge and understanding of a variety of risk management and risk assessment processes, particularly as they relate to the Standard and TRAs.

### **Contacts**

Phil Walker  
[Walker@Broadleaf.com.au](mailto:Walker@Broadleaf.com.au)

Dr Dale F Cooper  
[Cooper@Broadleaf.com.au](mailto:Cooper@Broadleaf.com.au)

Dr Stephen Grey  
[Grey@Broadleaf.com.au](mailto:Grey@Broadleaf.com.au)

Geoff Raymond  
[Raymond@Broadleaf.com.au](mailto:Raymond@Broadleaf.com.au)

Mike Wood  
[Wood@Broadleaf.co.nz](mailto:Wood@Broadleaf.co.nz)

Grant Purdy  
[Purdy@Broadleaf.com.au](mailto:Purdy@Broadleaf.com.au)

Dennis Goodwin  
[Goodwin@Broadleaf.com.au](mailto:Goodwin@Broadleaf.com.au)

Pauline Bosnich  
[Bosnich@Broadleaf.com.au](mailto:Bosnich@Broadleaf.com.au)