



**Trusted Information
Sharing Network**
for Critical Infrastructure Protection

Denial of Service/Distributed Denial of Service

MANAGING DoS ATTACKS

ADVICE FOR CEOs

July 2006

DISCLAIMER: To the extent permitted by law, this document is provided without any liability or warranty. Accordingly it is to be used only for the purposes specified and the reliability of any assessment or evaluation arising from it are matters for the independent judgement of users. This document is intended as a general guide only and users should seek professional advice as to their specific risks and needs.

EXECUTIVE SUMMARY

The Internet has become an indispensable business tool and its availability is often taken for granted. Organisations are increasingly dependent on the Internet through the adoption of email communications and interactive web-based services. However, with dependence comes weakness; the sudden and unexpected loss of Internet access and system function carries significant financial, social and security implications.

A Denial of Service (DoS) attack is a deliberate act exploiting a weakness to disrupt an organisation's functioning. The information in this paper will help you safeguard against a Denial of Service attack and outlines appropriate responses should one occur. It explains the issues, details some ramifications to your business and highlights questions to ask your Chief Information Officer (CIO).

This document has been developed by the IT Security Expert Advisory Group (ITSEAG), which is part of the Trusted Information Sharing Network (TISN)¹ for critical infrastructure protection. It is one of three parts:

- a CEO Paper;
- a CIO paper; and
- a full DoS analysis report.

As IT security governance is an important part of managing DoS attacks, it is recommended that these papers be read in conjunction with the *Best practice, management and governance for IT and information security guidelines for corporate and business* report issued by ITSEAG².

¹ TISN enables the owners and operators of critical infrastructure to share information on important issues. It is made up of a number of sector-specific Infrastructure Assurance Advisory Groups (IAAG), several Expert Advisory Groups (EAGs), and the Critical Infrastructure Advisory Council (CIAC—the peak body of TISN that oversees the IAAGs and EAGs). More on TISN can be sought from www.tisn.gov.au or by contacting cip@ag.gov.au.

The ITSEAG is one of the EAGs within the TISN framework. The ITSEAG provides advice to the CIAC and the sector-based IAAGs on IT security issues as they relate to critical infrastructure protection. Its members include academic specialists, vendors, consultants and some industry association representatives who are leaders in the information technology/e-security field. The ITSEAG Secretariat can be contacted on 02 6271 1595.

² Trusted Information Sharing Network. 2006. Best practice, management and governance for IT and information security guidelines for corporate and business. << URL to be provided >>

WHAT IS A DENIAL OF SERVICE ATTACK?

A Denial of Service attack occurs when a malicious person or entity limits legitimate access to computer systems and resources, causing interruptions to normal operations or, in a worst case scenario, a complete shutdown. While there are many ways to perpetrate a DoS attack, the most common approach is to flood an organisation's Internet connections with so much information that systems falter under the load. The more an organisation relies on Internet connectivity for critical communications, the more vulnerable it is to DoS attacks. The interconnected nature of modern communications means the ultimate impact of DoS attacks could be to:

- shut down email systems;
- impede website functionality;
- disrupt Voice over Internet Protocol (VoIP) telephony; and/or
- adversely affect networked computer systems across an entire supply chain.

At minimum, a DoS attack is a nuisance. For critical infrastructure organisations and commercial enterprises, the interruption of service, even for a few minutes, can result in a significant loss of productivity, money and reputation. While DoS attacks cannot be prevented, taking steps to protect an organisation against the threat is key to maintaining the availability of infrastructure. A strategy that consists of a risk-assessment program and adequate protection measures, combined with detection and response strategies, will ensure that your organisation is sufficiently prepared should an attack occur.

IMPORTANT ISSUES FOR CEOs AND BOARDS OF DIRECTORS TO CONSIDER

- **Financial**—DoS attacks can cause lost revenue, contractual violations, litigation costs, service provider expenses, incident handling and recovery costs, and even stock price fluctuations due to investor uncertainty. In a recent DoS attack, an online company calculated their losses to be almost \$100 000 per day. The final financial cost was well over a million dollars in lost revenue in addition to hardware and labour costs. The 2005 Australian Computer Crime & Security Survey reported one local respondent acknowledging an \$8 million loss that year resulting from a DoS attack.
- **Intangible**—Typically the intangible ramifications outweigh the monetary and are often overlooked. Some of the potential repercussions include third-party damage, lost productivity, brand damage and impacts on employee morale. The potential cost to the organisation arising from intangible losses should not be underestimated. Furthermore, a successful attack on a critical infrastructure service may result in substantial damage to public services, safety or confidence.
- **Crime**—Organised crime is increasingly using actual or threatened DoS attacks in extortion and commercial sabotage attempts. Attacks arising from political motivations or personal grievances are also becoming more common. Some attackers could be seeking to damage the image or brand value of the company.
- **Targets**—Some critical infrastructure targets are more vulnerable than others to a DoS attack, such as those with Internet-dependent infrastructure or high public visibility.
- **Assessment**—In order to assess an organisation's risk from a DoS attack it is important to focus on critical communications and processes. External entities that provide critical services to the organisation must be included in this assessment.
- **Plan**—DoS attacks are a fact of life online. It is important to plan for them by incorporating DoS into existing risk-management programs.

Why do DoS attacks occur?

A range of reasons exist for DoS attacks, including:

- retaliation for real or perceived slights or injustices;
- monetary gain (criminal extortion or competitive tactics); and
- the growing threat of political activism and cyber terrorism.

ISSUES TO RAISE WITH YOUR CIO

Supply Chain: Organisations today operate in an interconnected web of suppliers, outsourcers and customers, and each can be critical to the effective operation of the enterprise. When analysing the risks associated with DoS attacks, organisations must do more than just consider their own infrastructure. The ramifications of a partner undergoing a DoS attack should also be a consideration. Your organisation may not be the target but you can be affected by someone else's misfortune.

Q. How prepared are we and our trading partners to resist a DoS attack?

MANAGING DoS ATTACKS — ADVICE FOR CEOs AND BOARDS OF DIRECTORS

Assessment: The threat of a DoS attack is most effectively addressed as a risk-management issue and should be considered as an overall business risk, not a technical or operational risk. Risk management is a critical first step that allows you to decide the most appropriate technical and operational steps to mitigate the risk of DoS.

Q. What systems, connections, applications are most at risk?

Resources: Research into DoS has resulted in hardware, software and configuration strategies that help to resist DoS attacks. All of these come at a cost and the amount to be spent will depend on the outcome of a risk assessment. More resources can often help and service providers (including telecommunications carriers and ISPs) can be contracted to provide additional resources in times of crisis.

Q. Do we have the resources to implement an effective DoS mitigation strategy?

Employees: Both management and technical staff need to be aware of the threat of DoS attacks at the operational level, and possess the necessary skills and knowledge to protect, detect and react appropriately. In addition, all staff members need to have the necessary tools to enable them to effectively respond to an attack.

Q. Have we provided our staff with the knowledge and tools to detect and respond to a DoS attack?

Planning: The likelihood of a Critical Infrastructure organisation coming under a DoS attack in the future is higher than most organisations. Preparations for all contingencies must be made. The mitigation and response strategies developed cannot prevent some degree of loss of service. An understanding of how business will continue once service is denied is a vital component of the strategy

Q. What are our contingency plans in the event that service has been denied to us?

Testing: Some Australian critical infrastructure organisations have expressed interest in collaborating in a joint exercise, or in carrying out their own exercise, to share knowledge and experience, and to test for preparedness for cyber-attack.³

Q. Would our organisation benefit from collaborating in an industry-wide preparedness test? Is this organisation interested in conducting our own exercise?

The potential risk to an organisation of being subjected to a DoS attack is too great to ignore. The losses in productivity, money and reputation can be significant. A well documented plan to deal with the threat is a necessity.

³ The United States Department of Homeland Security in 2006 carried out an exercise dubbed Cyber Storm, testing the country's preparedness for cyber attack.

MANAGING DoS ATTACKS — ADVICE FOR CEOs AND BOARDS OF DIRECTORS

Further information is available at the TISN website (www.tisn.gov.au), including:

Reports

- Denial of Service and Distributed Denial of Service, Managing DoS Attacks
- Leading Practices and Guidelines for Enterprise Security Governance
- Critical Infrastructure Protection: Whose Responsibility is it?
- National Guidelines on Protecting Critical Infrastructure from Terrorism

Information for CEOs

- IT Security and Governance for Board of Directors and CEOs
- GPS—An Overview for CEOs
- SCADA—Advice for CEOs
- Security of Voice Over Internet Protocol (VoIP)—Advice for CEOs
- Wireless Security—Overview for CEOs

Information for CIOs

- Denial of Service /Distributed Denial of Service: Advice for CIOs
- CIO and CISO Practitioner Guidance: IT Security Governance
- Security of Voice Over Internet Protocol (VoIP)—Advice for CIOs
- Wireless Security – Overview for CIOs