Data breaches, resulting in costly and brand-damaging data loss events, have become big business for malicious hackers. Targeted attacks are on the rise, as are the associated “per-record” remediation costs. A recent study conducted by the Ponemon Institute reported that data breaches can cost organizations nearly two hundred dollars per exposed record. When the secondary losses from potential customer attrition and brand damage are considered, these costs can increase significantly.

Given the current threat landscape, one of the biggest challenges that organizations face today is how to balance the operational demands for information availability with the need to adequately protect that information from unauthorized disclosure. These are not mutually exclusive goals and Symantec understands the importance of maintaining a balance between information availability and information protection.

Service Overview
Symantec's Information Exposure Assessment provides customers with a holistic and data-centric view of their organization's information risk. By combining industry-leading advisory consulting services and data loss prevention technologies, Symantec is uniquely positioned to provide customers with not only a detailed analysis of their exposure to internal and external data breaches, but also a quantitative assessment of actual data loss risk across networks, web applications, storage and endpoints.

This combined approach allows for Symantec to deliver a detailed and comprehensive risk mitigation plans focused on priority data loss and data exposure concerns. The result is a detailed plan of action that includes guidance on addressing internal and external risks and recommended activities to reduce and eliminate areas of exposure across the entire organization.

Approach
Symantec’s Information Exposure Assessment is comprised of two primary focus areas: an Internal Analysis and an External Analysis. By leveraging the findings from the Internal Analysis to focus the External Analysis, the Information Exposure Assessment provides companies with a complete picture of information security risk. Importantly, the assessment results in a clearly defined and measureable remediation plan to address individual exposures within the context of the larger information risk profile.

- **Internal View:** Organizations gain a clear understanding of internal security exposures related to specific types of data within an organization, based on information discovery within a Data Loss Prevention assessment coupled with a targeted internal network penetration assessment conducted by security advisory experts.

- **External View:** Targeted vulnerability testing validates the existence of external security exposures and identifies ways to remediate.

Detailed Services Description
The Symantec Information Exposure Assessment combines consulting advisory services and industry-leading data loss prevention technologies to assess actual data loss risk and security vulnerabilities across networks, web applications, storage, and endpoints.

- **Critical Information Classification.** This step involves reviewing an organization’s key information classification levels and assigning specific data assets and asset categories to the appropriate levels within the information hierarchy. Traditional information classification models allow for public, private, confidential, and top-secret data categories to determine where information should be stored, how it should be protected, where it can be sent, and who should have access to it.
Overview

Symantec Consulting Services

Symantec™ Information Exposure Assessment

- **Critical Systems Classification.** In this step, systems are identified where sensitive information and data assets are stored, processed, managed, or viewed by internal and external resources.

- **Data Discovery Assessment.** In this step, a targeted data discovery scan locates and quantifies the amount of sensitive data residing on high-priority devices as defined in the Critical Systems Classification.

- **Data Loss Assessment.** The object of this step is to gain visibility into, and quantify, your organization’s risk of data loss based on the data protection policies as determined in the Critical Information Classification phase. This step identifies where sensitive information is being sent, who is sending it, and how often it’s happening.

- **Network and Web Application Penetration Assessments.** Using information gathered in the Data Discovery and Data Loss Assessments, a targeted vulnerability assessment is performed. This step identifies specific attack vectors that may be used by malicious users to gain access to your critical information and systems. It also provides insight into vulnerabilities that may expose critical information, the ease with which an attacker can exploit those vulnerabilities, the level of effort needed to remediate those issues, and the estimated business impact.

- **Information Exposure Assessment Summary.** The final step is the delivery of a summary report detailing the findings of internal and external information exposure risks. Quantitative data loss metrics are provided for the network, storage, and endpoints. The report also outlines high-priority information exposure concerns, and includes recommend key tasks and activities for a risk mitigation plan.

**Conclusion**

Symantec understands one of the biggest challenges that organizations face today is how to balance the operational demands for information availability with the need to adequately protect that information from unauthorized disclosure. By engaging in an Information Exposure Assessment, customers will gain invaluable insight and visibility into their current information exposure risks, and begin to proactively manage that risk in a coordinated approach.

**Visit our website**
http://enterprise.symantec.com

**To speak with a Product Specialist in the U.S.**
Call toll-free 1 (800) 745 6054

**About Symantec**

Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

**Symantec World Headquarters**

350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

Copyright © 2009 Symantec Corporation. All rights reserved. Symantec and the Symantec logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

12/09 20096091