Sensitive Information Leakage Survey
By Osterman Research, Commissioned by Entrust Inc.

Entrust Inc. commissioned Osterman Research to survey IT managers and decision makers in medium and large enterprise regarding their business use of various communication protocols and what vulnerabilities they believe they face regarding confidential or sensitive information leaking outside of the organization over those protocols.

The results show us that email is still the primary vehicle for communicating sensitive information into or outside of the organization, with 70% of respondents noting this. Instant Messaging was noted by 6% of respondents as containing most sensitive information, and FTP was cited by 12%.

Typically employees are not aware of security policies regarding the communication of sensitive corporate or customer information, and as a result this data is leaking outside of the organization, more often by accident than by malicious behavior. Specifically, the survey found that while 88% of organizations have a policy outlining the appropriate handling of confidential and private information, in over 55% of organizations less than a quarter of the employees have reviewed it in the last 6 months.

The frequency by which confidential and private information is suspected to be leaking outside of organizations is shocking, with 96% having experienced a sensitive data leak. The figure below shows how often organizations suspect this type of information is leaving the organization in violation of their policies.

Figure 1: How Frequent Sensitive and Private Information is Suspected to be Leaking Outside of their Organization.
The majority or organizations however, 83% believe that most information leakage is accidental, due in part to employees simply not knowing the policy or not realizing the information they are sending is sensitive.

The following chart indicates the types of information that the respondents were 'most concerned' about accidentally or maliciously leaking outside of the organization.

To address these concerns, organizations realize they must implement technology to assist them in detecting and reporting sensitive and private information leakage, and where possible either block it explicitly or secure it as it travels the network with technologies such as encryption.

The survey found the following approaches were noted as top priorities for organizations as they look to address sensitive and private information leakage:

- 59% Monitor and Block Email violations
- 51% Encrypt Email communications that contain sensitive or private information
- 36% Monitor Instant Messaging (IM) communications
- 32% Monitor FTP Transmissions
- 29% Monitor Web postings or Web Email

Report Methodology
The Entrust Sensitive Information Leakage market research is based on on-line survey findings collected by Osterman Research between November 18-28, 2005. A total of 140 respondents completed the survey. Survey respondents were made up from enterprise IT managers around the world. While the data collection was conducted on behalf of Entrust Inc, at no time were the survey respondents aware of our participation. The confidence interval of data collected is + or -5.56% with a 90% confidence level.

About Entrust
Entrust, Inc. [NASDAQ: ENTU] is a world-leader in securing digital identities and information. Over 1,400 enterprises and government agencies in more than 50 countries rely on Entrust solutions to help secure the digital lives of their citizens, customers, employees and partners. Our proven software and services help customers achieve regulatory and corporate compliance, while turning security challenges such as identity theft and e-mail security into business opportunities. For more information on how Entrust can secure your digital life, please call us at 888-690-2424, or send an e-mail to entrust@entrust.com. Visit us on the Web at www.entrust.com.