



The Insider Threat: Understanding the Risks & Defending the Enterprise



The virtual world moves at a pace that is much faster than the physical one. That same easy connectivity means today's companies must protect their networks while maintaining availability and security. Laptops, mass storage devices, email and the web are becoming increasingly important tools for internal attackers. Some postulate the issue is not just the ease and stealth with which mobility allows attackers to misuse the resources of an organization.

Sociologists believe there is actually a breakdown in the conscience's natural barriers that allows an attacker to carry out a threat. In addition, attackers can work from the safety of their home or a remote location, thus increasing their predisposition to go out and do something they should not do. Deloitte Touche Tohmatsu conducts an annual "Global Security Survey." The 2005 report surveyed senior security officers at the world's top 100 financial institutions. It found that insiders were often perpetrators of information theft and resource damage.

For large global financial institutions, the insider threat has surpassed external threats. About 35 percent of respondents said they had encountered attacks from inside their organization within the last 12 months, up from 14 percent in 2004. In contrast, only 26 percent confirmed external attacks, compared to 23 percent in 2004. According to industry analyst Gartner, 84 percent of insider incidents occur when insiders send confidential data outside the company. A major report released in June 2005, the "CERT® Insider Threat Study," analyzed both the behavioral and technical aspects of insider threats. The study found that the impact of nearly all insider incidents in the banking and finance sector from 1996 to 2002 was financial loss for the affected organization: in 30 percent of the cases, the financial loss exceeded \$500,000. Many affected organizations experienced damage in multiple areas.

CERT summarized typical incidents in the banking and finance sector as follows:

- Insiders were authorized users with active computer accounts
- Insiders had little or no technical expertise and exploited non-technical vulnerabilities such as business rules or organization policies (rather than vulnerabilities in an information system or network)
- Insiders devised and planned the incidents in advance, and others often had knowledge of the insider's intentions, plans, and/or activities
- Insiders executed their attacks physically from within their organization during normal business hours, using simple, legitimate user commands to carry out the incidents
- Most insiders were motivated by financial gain rather than a desire to harm the company or information system



- Insiders in this report fit no common profile:
 - 23 percent held a technical position
 - 13 percent had a demonstrated interest in "hacking"
 - 27 percent had come to the attention of a supervisor or co-worker prior to the incident



Insider incidents were detected by internal as well as external individuals however it is usually the lack of proof that deters them from acting. It can be difficult to stop the smart insider who is focused. However, it is honest mistakes by people within an organization that cause a large portion of the threats. This is a key point to keep in mind while developing a strategy for dealing with the insider threat. This briefing identifies the insider threat to the enterprise, the risks it poses, and the strategies needed to mitigate the problem.

Study Overview

The Ponemon Institute's annual benchmark study, begun in 2005, examines the costs organizations incur when responding to data breach incidents resulting in the loss or theft of protected personal information.

- To complete the study, benchmark surveys were sent to companies known to have experienced a breach involving the loss or theft of personal customer, consumer, or student data over the past year.
- Of that group, 31 companies agreed to participate by completing the survey. Results were not hypothetical responses to possible situations; they represent cost estimates for activities resulting from an actual data loss incident.
- Reported number of individual records breached ranged from 263,000 to 815,000 from companies in 15 different industry sectors.
- Survey shows that almost 30 percent of all data breaches are from external sources, including outsourcers, consultants, business partners, and contractors.

This table summarizes the 14 study participants by industry and source of data breach:

INDUSTRY	NUMBER	INTERNAL BREACH	EXTERNAL BREACH
Retail & Online Commerce	7	7	0
Financial Services	5	4	1
Hardware & Software	3	1	2
Services & Outsourcers	3	2	1
Health Care & Benefits	2	1	1
Pharmaceuticals	2	2	0
Insurance	1	0	1
Hotels	1	0	1
Airline	1	1	0
Education	1	1	0
Telecom	1	0	1
Utility	1	1	0
Automotive	1	1	0
Not Disclosed	2	1	1
TOTAL	31 100%	22 71%	9 29%