Risk Control Bulletin
The A B Cs of Information Risk

RISK CONTROL

CNA

The complexity of information systems in today's business world – even for relatively small businesses – is mind boggling. The risks to the data handled by these systems are equally complex. However, common causes of loss are being identified. The purpose of this article is to review the broad categories of information risks, as well as broad strategies for managing them.

Information Risk Classification

Information risks include threats to information technology systems, the intangible property handled by them and consequences of failure of these systems. These risks include first-party losses that would be sustained by the organization or third-party losses related to liability to others. Some examples of these risks are given below.

First-party Risks

- Loss of data
- Loss of business income
- Denial of service
- Virus/hacker/sabotage
- Theft of system resources
- Extortion

Third-party Risks

- Theft/disclosure of or damage to someone else's data
- Privacy injury liability
- Network security liability
- Content liability
- Spread of viruses or malicious code to someone else's system

In general, these are events that may compromise the confidentiality, integrity or availability of an organization's electronic data or otherwise cause a loss of system resources. These same events may create liability to others in regard to data of others that is stored, handled or processed by an organization.

Historical data on these causes of loss is limited. However, there is a growing public record of incidents related to security breaches of databases and the private information they contain. Analysis of data on these breaches provides insight into the causes of a much wider range of information-related losses.

Breaches of Sensitive, Non-Public Information

According to data available from the Privacy Rights Clearinghouse, physical theft, hacking into systems and accidental release are the leading causes of breaches of sensitive or non-public information.

Incident Frequency by Cause of Security Breach — All Industries*

354 Recorded Privacy Breaches

	% of Total
Physical Theft	36%
Hacking	26%
Accidental Release	20%
Lost Media	11%
Employee Act	6%
Social Engineering	1%

Records Exposed

Approximately 102.1 Million Total

	% of Total
Hacking	47%
Physical Theft	37%
Lost Media	11%
Accidental Release	3%
Employee Act	2%
Social Engineering	<1%

*Source: "A Chronology of Data Breaches." Privacy Rights Clearinghouse. May, 4 2007.

www.privacyrights.org/ar/ChronDataBreaches.htm.

Physical Theft and Lost Media

Physical theft of desktop PCs, laptops, PDAs, tapes, disks, USB drives or other devices and media create significant risks to the information stored on these devices. These incidents are the most frequent cause of privacy breaches. Physical theft also ranks second in terms of number of records exposed. The expanding use of portable devices and rapid increases in storage capacity warrant significant attention to how these devices and the data they contain are secured.

It should also be noted that the exposures related to lost media are the same as for physical theft. The separate category for lost media constitutes incidents related to poor tracking and physical control of media, such as back-up tapes. Unless steps are taken to protect the data on such misplaced media, the data they contain is vulnerable to unauthorized access.

Hacking

Unauthorized access to networks by hackers represents almost half of all records breached during the time period represented in the chart. Hacking ranks second in terms of frequency of occurrence. In addition to theft of information that can create privacy concerns, once unauthorized access is gained to a system, a hacker can perform a variety of malicious activities. These activities may include theft of an organization's intellectual property, destruction of data, sabotage and theft of system resources.

Accidental Release

The Privacy Rights Clearinghouse data on security breaches shows that accidental releases of confidential information occurs in a variety of ways. Much of the data was released in electronic form via the Internet, an organization's Web site or email.

Other releases are related to discarding equipment or media that was not properly sanitized to remove all traces of non-public information. Loose editorial and content controls can allow these types of breaches to occur and can also create other types of liability related to content published electronically. This includes liability related to claims of libel, slander and intellectual property rights infringement.

Employee Acts and Social Engineering

Some of the cited breaches indicate the specific involvement of rogue employees who gained unauthorized access to systems and information, or misused authorized access privileges. Also in evidence are social engineering techniques in which employees or others are manipulated into performing acts that facilitate a breach or divulging confidential information. While the frequency and severity of incidents in which these techniques are the primary cause of a breach is shown to be low, the overall impact should not be underestimated.

The preceding discussion is specifically related to causes of security breaches that resulted in or had the potential to result in identity theft and privacy liability. The same causes also result in a wide range of other types of first□ party and third party losses.

Risk Management Strategies

It is becoming increasingly clear that emerging risks associated with protecting data should be included in an organization's overall approach to risk management. In to-

day's data-focused world the loss of a valuable information asset can be just as damaging as a fire that consumes a warehouse full of tangible property or accidental physical harm caused by a company's operations.

Risk management strategies to protect the confidentiality, integrity and availability of data follow the same general pattern as for other risks: identify the exposures, implement controls, and handle the residual risk via contractual risk transfer and insurance. Contractual risk transfer to service providers, vendors and other third-parties with access to your client data is very important. An estimated 30% to 40% of all breaches involve third-parties who have compromised in some fashion their client's data.

While a detailed discussion of risk management strategies is beyond the scope of this article, the following risk controls represent some of the minimum pro-active steps necessary to help protect your organization.

Anti-Virus & Firewalls

- Employ anti-virus software on all computing devices
- Automatically update anti-virus software at least daily
- Automatically scan and filter e-mail attachments and downloads before opening files
- Automatically receive virus and threat notifications from the United States Computer Emergency Readiness Team
- (US-Cert), SANS Institute or a similar provider
- Securely configure firewalls other than a default configuration
- Configure networks using multiple firewalls (or equivalent) to separate back-office operations from Internet-facing operations

Network and Data Security

- Back up network data and configuration files daily
- Store back-up files in a protected location
- Allow remote access to the network only if it is via a VPN or equivalent system
- Monitor network platform vendors at least daily for availability of security patches and upgrades
- Test and install security patches and upgrades within 30 days of availability, preferable within seven days
- Always lock server room or otherwise limit access to authorized personnel

Policy & Response Plans

- Promulgate a security policy to all employees and contractors
- Have a tested disaster recovery plan that includes recovery from data center disasters
- Have a tested security incident response plan that addresses both direct (e.g. hacking) and indirect (e.g. virus) attacks upon your network