Knowing What You're Up Against:
3 Leading Causes of Information Breaches

CNA
We can show you more.®

PROFESSIONAL SERVICES

The complexity of information systems in today's marketplace can be just as daunting as the risks to the data handled by these systems. However, common causes of loss are being identified, making it easier to take preventative control measures. It's important to know the broad categories of information risk as well as the leading causes of breaches to better protect yourself and your business from cyber breaches.

Classifying "Information Risk"

Information risk includes 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 your organization, or third-party losses related to liability to others. Some examples of these risks include:

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 events may compromise the confidentiality, integrity or availability of your electronic data – or otherwise cause a loss of system resources. These same events may create liability to others, such as your clients, in regard to data that is stored, handled or processed by your organization.

When it comes to breaches of non-public information, according to data available from the Privacy Rights Clearinghouse, physical theft, systems hacks and accidental release are the leading causes of breaches of sensitive or non-public information.

Physical Theft and Lost Media

Physical theft of desktop PCs, laptops, tapes, disks, USB drives, or other devices and media create significant risks to the information stored on these devices. In fact, physical theft is the most frequent cause of privacy breaches and ranks second in terms of number of records exposed.[1]

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. For example, if the laptops used by employees at a company are poorly tracked, and a laptop goes missing, it would be extremely difficult to pinpoint who last had access to the laptop and find out where that lost media could be located.

Additionally, all data should be consistently backed up on a separate device or at an off-site location, and all devices should be encrypted. Encryption mitigates most of the liability when a device is lost.

[1] "A Chronology of Data Breaches." Privacy Rights Clearinghouse. May 4, 2007.

Systems Hacks

Unauthorized access to networks by hackers represents nearly half of all records breached.[2] Hacking ranks second in terms of frequency of occurrence, just behind physical theft. 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 your intellectual property, destruction of data, sabotage and theft of system resources.

Accidental Release

Accidental release of confidential information occurs in a variety of ways – via the Internet, your website, an employee's email, or even misplacing information into postal mail or mailing information to the wrong recipient.

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.

Additionally, while some releases involve rogue employees who gained unauthorized access to private information, many employees simply misuse authorized access privileges. Social engineering techniques, for instance, manipulate employees into performing acts that facilitate a breach or divulge confidential information.

Knowing the risks you face will make it easier to develop your risk management strategy. The unfortunate fact is that not all breaches can be blocked. However, there are many ways business owners can lessen their risk of getting hacked. Learn how in my blog series.

Additional Resources

Holding Your Business' Data Ransom

Is your Data at Risk? Who Are Hackers and What Are Their Methods of Attack?

Hackers – Past, Present and Future

The above resources can be found on CNA.com.

[2] Ibid.

To learn more about how to keep your business protected, visit www.cna.com.

The information, examples and suggestions presented in this material have been developed from sources believed to be reliable, but they should not be construed as legal or other professional advice. Consultation with competent legal counsel and/or other professional advisors before applying this material in any particular factual situation is recommended. This material is for illustrative purposes and is not intended to constitute a contract. Please remember that only the relevant insurance policy can provide the actual terms, coverages, amounts, conditions and exclusions for an insured. All products and services may not be available in all states and may be subject to change without notice. "CNA" is a service ma rk registered by CNA Financial Corporation with the United States Patent and Trademark Office. Certain CNA Financial Corporation subsidiaries use the "CNA" service mark in connection with insurance underwriting and claims activities.
PS3306C
FL GRAF SS 010617