



Enterprise Security Office Monthly Security Tips

NEWSLETTER

JUNE 2008

Volume 3, Issue 6

Data Breach

There are stories almost daily in the media about major security data breaches. These involve the theft of Social Security numbers, credit card numbers and other information that can be used to identify an individual. These thefts are often connected with attempts to steal identities for monetary gain. In response to this growing threat, the Oregon Legislature passed the Oregon Consumer Identity Theft Protection Act in 2007.

Knowing how to protect your personal information, as a consumer, is very important. Past issues of the Monthly Security Tips newsletter have presented information to help you protect your information and to respond in the event you think your information has been stolen. But it is important to recognize that theft of personal information is just one type of data breach. As custodians of information we receive as part of our daily duties, we must also be aware what information is considered to be sensitive, how it can be compromised, and what we can do to protect it.

What is a Data Breach?

Data breach generally refers to instances where information has been subject to unauthorized access, often where the information is lost, stolen or hacked into. This is of particular concern when that information is private, sensitive, or confidential. Organizations and individuals have the responsibility to protect the information in their care and proper safekeeping of this data is vital. Failure to do so can result not only in a breach, but also result in damage to reputation, significant fines or loss of revenue, and other negative consequences.

Data breaches are occurring all too frequently, and they can occur in large or small organizations, in the public and private sectors. The scope of this issue can be evidenced by the fact that more than 229 million records nationwide have been involved in personal information breaches alone since February 2005. This figure represents only those breaches that have been reported, so it may reflect only a portion of the actual data breach occurrences. This is an issue that everyone must be aware of and take steps to mitigate.

In addition to data breach concerns, we must also recognize that data manipulation is a potential threat. If we cannot trust the integrity of our data, and know that it has not been altered inappropriately, our ability to carry out our mission and serve our customers becomes impaired.

Breaches involve all types of data, not just personally identifiable information that is often used for identity theft. Some examples of data that must be protected include:

- Customer or employee information with names, addresses, Social Security numbers, credit card numbers, passwords and other identity-related information
- Intellectual property including computer code
- Financial information
- Health records
- Log-on credentials, such as user names and passwords, for sensitive systems
- School records such as student grades

How is Data Compromised or Disclosed?

External hackers often attempt to steal information. Attackers may use social engineering, phishing or other similar attempts to gain access. These activities can translate into very large sums of revenue for those in the organized crime world.

While very sophisticated techniques are sometimes used to steal sensitive data, one of the most common threats comes

from within the organization. According to Deloitte's *2007 Global Security Survey*, 65 percent of respondents reported repeated breaches. Of those incidents, 18 percent stemmed from unintentional data leakage. The report also indicates that some of the surveyed data breaches went undetected for extended periods.

The loss or theft of data is not limited to electronic data loss or computer hacking. Other possibilities include physical loss of hard copy documents, theft or loss of laptops, tapes and flash-drive devices or improper disposal of hard copy documents.

Are there Laws or Regulations to Protect Data?

There are numerous laws and regulations to regulate how organizations must handle and protect sensitive information. Some of the most notable include the following:

- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Payment Card Industry (PCI) Security Standard
- Gramm-Leach-Bliley Act (GLBA applies only to financial institutions)
- Sarbanes-Oxley Act (SOX applies only to public companies)
- Oregon Consumer Identity Theft Protection Act (Senate Bill 583, 2007 Legislative Session)

There are Breach Notification Laws currently in place in forty-two states and the District of Columbia which govern the notification of an individual whose personal information has, or may have been disclosed.

What Can I Do?

Organizations and individuals must take proactive measures to minimize the risk of data breach. Everyone in an organization has a role in protecting information. The following are examples of steps you can take to help prevent data disclosure:

- Follow your organization's information security policies and procedures;
- Know how your organization has classified information and adhere to the appropriate controls in place;
- Follow proper procedures for the destruction or disposal of media that contain sensitive data;
- Participate in security awareness training.

Remember, information security is everyone's responsibility.

Online Resources

To learn more about protecting information visit the following online resources:

- **Monthly Security Tips:** <http://oregon.gov/DAS/EISPD/ESO/Pub.shtml>
- **US CERT:** http://www.us-cert.gov/reading_room
- **OnGuard Online:** <http://www.onguardonline.gov/topics.html>
- **Privacy Rights Clearinghouse:** <http://www.privacyrights.org>

Brought to you by:



www.msisac.org