

Control Essentials

Volume II, Issue I

March 2005

Enterprise Risk Management provides the following services:

- Information Security Design and Implementation
- Vulnerability Assessments
- Penetration Testing Studies
- Security Remediation
- Internal Information Systems Audits
- Application Control and Security Services
- Business Continuity Plan (BCP) Services
- Attestation and Assurance
- Compliance with Federal Laws and Regulations

Identity Theft

Identity theft refers to all types of crime in which someone wrongfully obtains and uses another person's identification information for the purpose of fraud or other criminal activity. Unlike certain crimes that are specific to particular types of property and locations, identity theft is committed in every place associated with daily life. Moreover, the growth in the use of digital data and of computers and devices that transmit or store sensitive information, means that identity thieves can obtain that information without ever coming into physical proximity with the individuals whose data they are stealing.

According to a survey performed by the Federal Trade Commission (FTC) about consumer complaints, identity theft is considered to be the nations top consumer complaint.

The survey shows that identity theft accounted for approximately 40 percent of the 635,173 reported consumer fraud complaints. Additionally, credit card fraud was the most common form of identity theft reported.

The pie chart summarizes the top categories of consumer fraud complaints as a result of the survey.

The victims of identity theft come from every age group and all segments of society; however, the majority of victims appear in segments of the population with good or potentially good credit ratings.



Identity thieves use a variety of methods to gain access to personal information. Among these methods, we can mention the following:

- Rummaging through trash, whether commercial or residential, to find items of use that have been discarded. This method is known as "dumpster diving".
- Stealing credit and debit card numbers as your card is processed by using a special storage device. This method is known as "skimming".
- Hacking into an organizations computers.
- Stealing records from an employer.
- Stealing personal information from your home.
- Stealing wallets and purses containing identification and credit and bank cards.
- Stealing email including bank and credit card statements, pre-approved credit offers, or tax information.
- Phishing, Spoofing and Pretexting. Consumers receive emails that appear to belong to a legitimate business such as a financial institution but, in fact, redirect the user to a fake web site. This web site collects all the information the user sends.

Identity Theft (continued)

They are two main impacts caused by identity theft. The first impact is the direct cost of the financial loss. The second impact is the indirect cost of the type of harm the identity theft creates on his/her victims such as credit ratings and reputation damage. Moreover, the victims could be mistaken as criminals by law enforcement.

Attack prevention

To prevent identity theft, it is vital that businesses enhance and secure their information handling processes. A clear understanding of the classification of information is imperative before assessing processes. When assessing information handling security, the following areas must be considered:

Acquisition: The method in which the information is gathered. Adding information in paper form differs from adding information in an e-form on a web site.

Storage: Where this information will be stored? What logical and physical security mechanisms are in place?

Access: Who needs access to the information? This area is dependent on the type of storage since different types of mechanisms require different types of access.

Disposal: How the information is disposed of? Based upon how the information is stored, i.e. magnetic or physical form, disposal methods should be appropriate.

Distribution: How the information is handled? Is information transferred from one employee to another? How much information do employees need?

In addition to the assessment of the aforementioned areas, it is important to provide employees security awareness training.

Law enforcement

In 1998, the federal government passed 18 U.S.C. 1028 "The Identity Theft and Assumption Deterrence Act of 1998" which made identity theft a federal crime. In most instances, a conviction for identity theft carries a maximum penalty of 15 years imprisonment, a fine, and forfeiture of any personal property used or intended to be used to commit the crime.

Schemes to commit identity theft or fraud may also involve violations of other statutes, such as credit card fraud, computer fraud, mail fraud, wire fraud, financial institution fraud, or Social Security fraud. Each of these federal offenses is a felony and carries substantial penalties - in some cases, as high as 30 years in addition to fines.

Conclusion

Despite the fact that many organizations believe that identity theft is a customers' problem; the truth is that the crime depends on how the identity thieves obtain the information. If customer information was obtained due to company negligence such as the lack of security controls, where the information is stored, or instances where the helpdesk discloses more information than is necessary; organizations are responsible. The occurrence of identity theft due to the lack of proper controls and processes can cause financial loss as well as impact an organization's reputation.

If you are interested in obtaining more information on how ERM can assist you in preventing the loss of information that could result in identity theft, please contact us at (305) 447-6750 or at info@emrisk.com. We would be more than happy to provide additional information on how we can assist in your compliance efforts, the resumes of our professional team members, and a listing of client references. We can also provide you a comparable listing of our billing rates which are significantly lower than those offered by other accounting and consulting firms.

Hope to hear from you soon!