An Employee's Guide to Safeguarding Sensitive Information Properly

Available end of June 2012 on ebook!

12 Keys Every Employee Should Know

An Employee's Guide to Safeguarding Sensitive Information Properly

Just* SSIP*it! Is owned by Stealth Awareness, Inc.

Published by Stealth Awareness Inc. You can visit the author at www.stealthawareness.com

For more information or to book an event contact the author, Sean Lowther at info@stealthawareness.com

Cover designed by Sean G. Lowther

ISBN: 9781620959626

Also by Sean G. Lowther

Techno Security's Guide to Securing SCADA: A Comprehensive Handbook on Protecting the Critical Infrastructure

Low Tech Hacking: Street Smarts for Security Professionals

A Manager's Guide to Safeguarding Sensitive Information Properly

Holding the Moon in the Palm of Your Hand

DEDICATION

To all those who understand that safeguarding sensitive information properly is an imperative to securing not only our personal information, but that of the customers we serve, the employees we work with, the intellectual and sensitive information of the company we work for, the businesses we support, and vendors who support the mission of our company to provide exceptional products and services, and by exhibiting the trust they place in us to safeguard sensitive information properly.

Introduction

There is a risk in America that has reached epidemic proportions. It stems from employees working across our country in large and small companies who are entrusted to, and yet fail, to safeguard customer, employee, business, company, and other sensitive information properly, because they have not been given adequate guidance.

These risks are seen when a laptop that has unencrypted sensitive information is lost or stolen, or when sensitive documents are placed in regular trash versus designated bins for destruction. It ranges from company sensitive conversations overheard in public places to leaving sensitive documents on the copier for unauthorized individuals to view.

We never know when an individual will call or show up at the office disguising him or herself as an employee or vendor looking to extract sensitive information from unwitting employees. It's easier to ask for network IDs and passwords than to hack into network systems. These individuals, known as social engineers, are very adept at conning sensitive information out of unsuspecting employees who do not understand or suspect the risk. Each piece of information they acquire could result in serious damage to the company you work for and possibly your job too.

Safeguarding sensitive information properly (**SSIP**) is your responsibility as an employee, whether or not your management has instituted a viable information security awareness program. What you will find in this guide is universal with the possible exception of your company's password and social media guidelines. Make note where your company differs from what has been expressed or implied in this guide.

Just SSIP™ it!

Safeguard Sensitive Information Properly

Table of Contents

Key 1: What is sensitive information?

The basic principles of safeguarding sensitive information are:

1) **Confidentiality** - Persons should only have access to information they rightfully are approved to view.

2) **Integrity** - Only authorized persons should modify information.

3) **Availability** - Information should be accessible to authorized persons when they need it.

You should discuss with your manager how to safeguard sensitive information as it pertains to your job function. For our purposes, it is important that you understand the principles and how they are applied to safeguarding:

• Customer information

• Business information

• Employee information

• Company information

• Vendor information

Let's look at each type of sensitive information.

Customer Information

Customer sensitive information is non-public, such as Social Security Numbers, account numbers and private financial information. Any information or combination of information that would allow someone to commit identity theft or fraud is considered sensitive.

Business information

A business is any company with which your company conducts business as a provider of services or products. Examples of sensitive business information include: non-public financial information about the company or transactions with that company; information your company might be aware of that, if exposed, would result in harm to that company, such as knowledge of new products before their release, or competitive business strategies.

Employee information

Your company maintains sensitive information about its employees, including personal information and other employment details. Income, benefits information, Social Security Number and other identifying information are considered sensitive. How many times in the last several years have there been stories about stolen laptop computers with military, student, employee or customer

This is the end of the preview. An Employee's Guide for Safeguarding Sensitive Information Properly can be ordered through your favorite ebook provider after June 30, 2012.