

Information Security for Business

Protecting Sensitive Data



Leslie Fuentes
Director of Information Technology
October 15, 2008

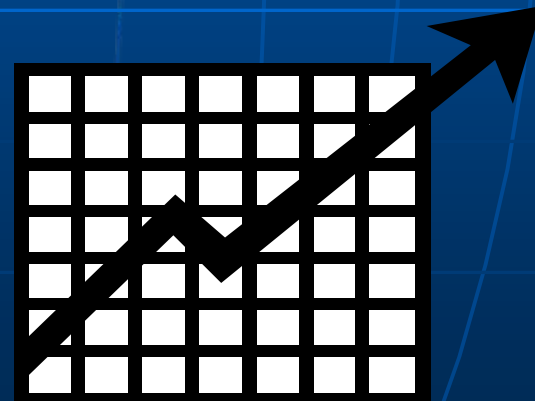
The Latest Statistic

2008 Computer Security Institute Survey*

- The most expensive security incidents involved financial fraud
- Average cost per incident \$300K
- 27% has experienced a targeted attack
- ✓ • Most businesses had or were developing a security policy

Security Plan Benefits

- Avoid Embarrassment
- Avoid Repair costs
- Avoid Misinformation or worse
- Avoid Loss of (eCommerce) business
- Maintain Trust of Trading Partners and Customers



Data Security Plan

5 Key Principles

1. Take stock
2. Scale down
3. Lock it
4. Pitch it
5. Plan ahead



1. Take Stock

Know what personal information you have in your files and on your computers

- Where stored
- Who has access
- What kind of information
- How do you receive personal information

Know Applicable laws & regulations

- Gramm–Leach-Bliley act (GLBA)
- Fair credit reporting act
- Federal Trade Commission Act
- Payment Card Industry Compliance (PCI) Standards

2. Scale Down

Keep only what you need for your business

- Use SSN only if required for lawful purposes
- Shorten/truncate credit card # on customer receipts
- Avoid keeping customer credit card information
- Dispose of sensitive data as soon as possible
- Develop a records retention policy and know your legal requirements for retention and disposal

3. Lock It

Protect the information you keep by physical and electronic security

- Keep paper files, CDs, tapes, disks, drives and back ups with personal info in locked room or cabinet with limited access
- Require employees to log off and put files away after work
- Install access controls for the building
- Maintain off site storage & limit access
- Encrypt sensitive information & track deliveries
- Identify & lock down all computers and network access points to sensitive information including wireless devices, laptops & e-mail
 - Install firewalls, strong passwords & lock down websites

4. Pitch It

Properly dispose of what you no longer need

- Paper – shred, burn or pulverize
- Computers – use wipe utility programs
 - Remember to remove files if a computer is moved to another employee
- If you use consumer credit reports you may be subject to FTC Disposal Rule

www.ftc.gov

5. Plan Ahead

Create a plan for responding to security incidents

- Designate a sr. employee to coordinate and implement response plan
- Computer compromise – disconnect immediately
- Investigate incidents immediately
- Report incidents as needed to customers, law enforcement, credit bureaus, etc. & consult your attorney

Resources

- www.hampton.gov/
 - City of Hampton website with this presentation
- <http://www.onquardonline.gov/default.aspx>
 - Security resource from the federal government and technology industry
- www.staysafeonline.info
 - Nat. Cyber Security Alliance For small business, home users.
- www.asbdc-us.org
 - Security Guide for Small Biz
- iase.disa.mil
 - Information Assurance Support_Free training materials, security configuration guides
- www.isalliance.org
 - Common sense infosec guides (for Senior Managers, Home Users, Small Biz)
- irtsectraining.nih.gov/
 - Free online-information security training – National Institutes of Health
- www.ftc.gov
 - Federal Trade Commission infosec info