Better Business Bureau®

Security & Privacy — *Made Simpler*™

Manageable Guidelines to Help You Protect Your Customers' Security & Privacy From Identity Theft & Fraud

Supported By

VISA

IBM

EQUIFAX

verizon wireless

THE WALL STREET JOURNAL.

ebay

PayPal

PRIVACY & AMERICAN BUSINESS

Security and privacy expertise contributed by Dr. Alan F. Westin and Dr. Lance J. Hoffman

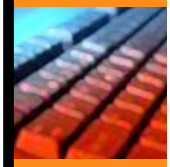
Published March 2006

Security & Privacy — *Made Simpler*™

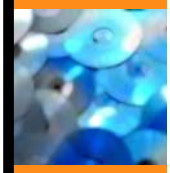
User's Guide

No matter what type of business you are in, you probably collect, store and share information about your customers. Whether it is providing a necessary service, completing a financial transaction or creating a mailing list, customer data has become a key currency of today's information-based economy.

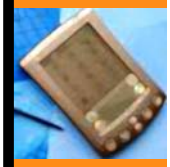
As a business owner, you make important strategic decisions that affect your bottom line. Each day, how you manage the security and privacy of the data you collect has become a core part of those strategic business decisions, because it can influence the success or failure of your business.



Data security and privacy management may appear complex and overwhelming, but you really don't need to become a privacy and security expert to manage it. All you need to do is to acquire the basic understanding of the issues and the business tools that will protect your customers…and your business.



Security and Privacy — *Made Simpler*™ is your Guide to getting your arms around many of today's data security and privacy challenges that affect small businesses, including:



- Recognizing attempts at theft and fraud.
- Understanding the importance of offline *and* online security and privacy practices.
- Developing a security and privacy policy, training your employees to comply with it, and communicating it to your customers.
- Handling, managing and protecting sensitive customer information.
- Managing employees as they interact with customers and their personal data.
- Credit card/debit card security—both during and after the actual transaction.
- Taking advantage of the latest technologies without compromising data security.
- Conducting international transactions securely.

Security and Privacy — *Made Simpler*™ advises you on how to incorporate basic security and privacy practices into your everyday business operations, offering you options, tips and advice that are right-sized for smaller businesses and will help you get started.

It is not intended to provide specific legal advice. The information is crafted—but not guaranteed—to be accurate, complete and up-to-date at the time of publication. Some of the information may not apply in your state or your particular line of business. Therefore, it is wise to consult an attorney familiar with the law in your jurisdiction and with your industry.

Security and Privacy — *Made Simpler*™ was developed through a partnership between the Better Business Bureau, a leader in promoting trust between businesses and the customers they serve, and Privacy & American Business, a leader in consumer and employee privacy and data protection issues and education.

This Guide is made possible through the support of corporate sponsors—industry leaders who are committed to the success of their small business customers.

Better Business Bureau®

Security & Privacy — *Made Simpler*™

PRIVACY & AMERICAN BUSINESS

Security is a complex issue.
You can manage it.
This Guide will help.

Click here for more security and privacy tools and resources for small business.

www.bbb.org/securityandprivacy

- *85% of Americans are worried about becoming victims of identity theft.*
- *58% of Consumers say if they were confident a business followed its security and privacy policies, they would be likely to recommend that business*

When your customers know you treat their personal information with the care it deserves, they will become more loyal and active customers.

Supported by:

VISA IBM EQUIFAX verizon wireless THE WALL STREET JOURNAL. ebay PayPal

1. Customer Data Security & Privacy—A Key To Your Success

Customers Care – You Should, too

When your customers know that you treat their personal information with care and apply good security and privacy practices, their trust and confidence in your business will grow.

You're Responsible For Customer Data

Businesses of all sizes—not just the big corporations—are held responsible for complying with federal and state customer data security and privacy laws. Here is a sample of how existing privacy laws may affect your small business:

Security & Privacy Drive Consumer Purchasing Decisions

- 85% of Americans are worried about becoming victims of identity theft.
- 64% of consumers say they had decided not to buy a company's product or service because they did not know how the company would use their personal information.
- 58% of consumers say if they were confident a business followed their declared security & privacy policies, they would recommend that business to family & friends.

Source: Privacy & American Business.

Here is a snapshot of existing federal privacy laws with which your small business might need to comply:

- *All small businesses* must comply with the federal and state Fair Credit Reporting Act (FCRA) when seeking to obtain consumer reports, such as credit reports and employment reports, about potential customers and employees.
- *Many small businesses in the healthcare field* must follow the privacy requirements of the federal Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and its data security requirements.
- *Small financial businesses* must comply with rules established by the federal Gramm-Leach-Bliley (GLB) Privacy Rules and Safeguard Rules and the federal banking agency guidance under GLB. Companies that need to comply with GLB include those that might not necessarily think of themselves as "financial," such as automobile dealers, tax planners, and some travel agents.
- *Currently, twenty-three states* have laws on reporting data breaches (outlined on page 19 of this Guide), with potential penalties for security lapses that apply to both large and small businesses.

As a business owner, it is your responsibility to stay current on privacy and security laws affecting your business…and your customers.

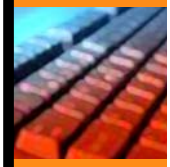
An Ounce of Prevention …

Establish good security and privacy practices now. The alternative is decidedly distasteful. If you have a data breach resulting from weak security practices, you and your business can face lawsuits from federal or state agencies or your customers. The Federal Trade Commission (FTC) recently sued 12 companies it accused of having inadequate data security practices in violation of federal law. Lawsuits stemming from inadequate security practices can erode business equity, consumer trust and, ultimately, your bottom line. Even if you don't face legal action, your good reputation could be significantly compromised.

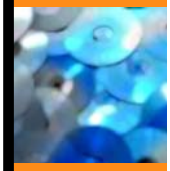
2. Security Challenges Facing Small Businesses

Firewalls Are Not Enough

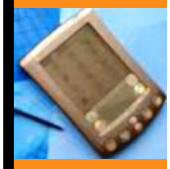
In today's tech-heavy business world, you might think that the right combination of hardware and software will prevent data security and privacy exposures. But technology is just one piece of the security and privacy equation. Effective policies, along with proper employee training and business-wide implementation, are the other parts.



Suppose you've equipped your computer with the latest network security software—firewalls, encryption—and you think you've deployed strong security tools. One day a "customer" calls your business to ask what credit card you have on file for his "account." He gives his "name" and "address" to an employee who then looks up the "customer's" information on your computer. Your employee reads the credit card number to the caller.



But the caller is not a "customer." He is a criminal who found the name and address of one of your customers in a trash bin. This happens. To prevent it, you need a data security plan that includes simple steps, such as properly verifying a caller's identity, and employee training. Software alone can't prevent employee error. Employee training can.



Modern technologies, such as e-mail, e-commerce, and cell phones, have given us wonderful new tools to do business more effectively and efficiently. They have also created new layers of security that businesses need to secure to protect their customers' information. If you use these new tools, you must also take reasonable steps to secure them.

Security & Privacy Challenges Facing Small Business

- Customer and business ID theft.
- Data loss and theft.
- Noncompliance with federal and state data protection laws.
- Employee fraud and theft.
- Loss of trust ... and customers.
- Costly lawsuits stemming from sloppy security practices.
- Computer and hardware damage from viruses.

3. Developing Your Own Data Security & Privacy Plans

Find Your Weak Spots

Take a few moments with a blank piece of paper and a pen, or at your keyboard. List all the different ways your business collects, stores and uses personally identifiable customer and business information. Now list who handles or has access to the information—employees, relatives, customers, service providers or visitors. Personal information may include names, addresses, account numbers, Social Security numbers, credit/debit card numbers and phone numbers, as well as account patterns and transaction records.

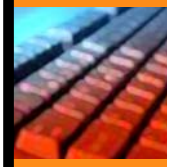
Anyone who appears on your list is a data handler and should play a significant role in protecting sensitive information. They need to be properly trained to follow your security and privacy policies and practices.

You may want to involve managers or employees from each business area in this

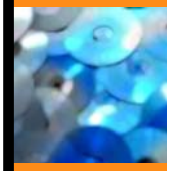
exercise, to be sure that you are not overlooking any potential security weak spots. Making your employees a part of the security and privacy planning process will make them feel like valuable contributors to the team, and will also make it easier for them to remember your policies and follow them on the job.

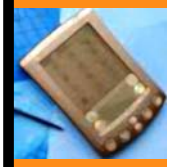
One Size *Does Not* Fit All

All businesses are not alike. Review your security and privacy issues in light of your particular business and its operations, identify weaknesses, and take stock of your current ability to address them.



You may discover areas where you need input from a lawyer or technology consultant. It is important to be fully informed about your business' security risks so you can make the most appropriate, reliable and cost-efficient choices for your business.





Security & Privacy Reality Check

- Do you transact business on the Internet?
- Do you collect names, addresses, phone numbers, e-mail addresses or Social Security numbers or other personal information about your customers or employees?
- Do you accept credit or debit cards?
- Do you share customer information with other companies?
- Do you engage in direct mail marketing or telemarketing?
- Are you storing customer information for any period of time?

If you answered "yes" to any of these questions, your small business is in serious need of a data security and privacy plan.

4. Creating & Communicating Your Security & Privacy Policies

Once you identify your security needs, you can begin to write a security and privacy policy for your comp any. Your security and privacy policy tells your customers how you will treat their personal information—how you will collect it, use it, and keep it secure. It should also give your customers the ability to communicate to you if they wish to receive ("opt-in") or not receive ("opt-out"), "subscribe" or "unsubscribe" information from you and how they wish to receive marketing communications (e-mail, US postal mail, etc.). Smart companies offer meaningful privacy choices, and effectively carry them out. Those that don't, risk losing their customers.

Resources to Help You Write a Policy

- The Privacy Planner from BBB*OnLine* can help you generate a simple, but solid online privacy policy for your business **http://www.privacyplanner.com**.
- The Direct Marketing Association (DMA) offers a small business-friendly online privacy policy generator **http://www.the-dma.org/privacy/privacypolicygenerator.shtml.**

How to Communicate Your Policies to Your Customers

Once you have a written policy that accurately describes your intended actions with customer data, it is wise to communicate these policies to your customers.

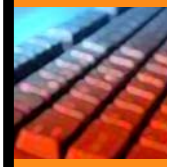
- Post it on a prominent sign in your store or office.
- Give customers a copy of it when they complete a transaction with you.
- Post it on the homepage of your web site.

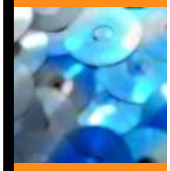
- If your customers have agreed to receive e-mail notices from you, tell them about your security and privacy notice in an e-mail, and let them know where they can find the full notice.
- Mail it to your customers as a separate promotional piece.

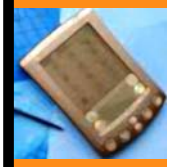
Posting a Security & Privacy Policy Provides a Competitive Advantage

Having and following a security and privacy policy will:

- Increase the trust and confidence your customers have in your business. When they know that you plan to use their information carefully and keep it secure, they will be more likely to share it with you.
- Help distinguish your business from your competition.







Prominent Security & Privacy Policies Build Businesses

- 89% of consumers felt more confident in giving personal information to a business that had a detailed but readable privacy policy.
- 58% of consumers said that if they were confident a business followed the privacy policies it presented, the consumer would be likely to recommend the business to family and friends.

Source: Privacy & American Business Study

5. Spotting Cyber Criminals

The number and sophistication of online fraud attacks is increasing. Here are some ways criminals attempt to get sensitive information from computers and individuals:

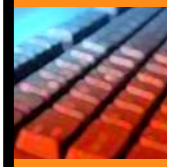
- *Viruses:* man-made programs or pieces of code that are loaded onto your computer without your knowledge. Viruses result in a wide range of disruptive consequences on a computer or network, including the deletion or corruption of files. New viruses are introduced to the Internet every day.
- *Spyware:* software that secretly collects information from a computer, such as what Internet sites are visited and what key-strokes (including passwords and credit/debit card numbers) are entered. Spyware transmits that information to a third party for a variety of uses, ranging from presenting tailored advertising or general spam to credit/debit card fraud and ID theft. *Spyware is often installed on your computer as part of a downloaded application or via a downloaded e-mail attachment.*
- *Phishing:* uses fake e-mails and web sites that closely replicate their authentic counterparts to trick recipients into "verifying" their personal information.
- *Pharming:* redirects an individual's web site request to a fraudulent site that closely replicates its authentic counterpart.
- *Keyloggers, Bots, Trojans and more:* applications that may appear to be benign or even helpful, but are actually destructive to files on your computer. These introduce viruses or malicious code onto your computer that can be programmed to execute any number of disastrous actions, and send sensitive information to a third party.

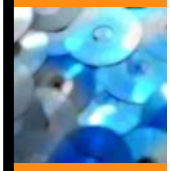
Consider installing a web browser tool bar to help protect you from known phishing web sites. Earthlink offers such a free tool, called ScamBlocker, at:
http://www.earthlink.net/software/free/toolbar.

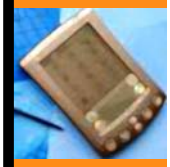
eBay also offers an anti-phishing and account protection toolbar that alerts users when they're on a potentially fake eBay or PayPal site **http://pages.ebay.com/ebay_toolbar/**.

Ways to Avoid Being a Victim of Online Fraud

- Always verify whom you are doing business with before revealing personal information.
- Ensure your browser is current with all security patches installed.
- Use anti-virus and anti-spyware software, and keep it updated.
- Be suspicious of any e-mail with "urgent" requests to validate or verify personal information.
- Don't download anything that comes from a source you don't know. This includes e-mail graphics, screen savers, free software, etc.
- Don't fill out any forms that come to you in an e-mail and request personal information, unless you definitely know and trust the source.
- Don't allow your children to use your business computers. Children are not aware of online threats, and can download items without considering what might be attached to them.







6. Fighting Identity Theft

How Identity Theft Happens

ID and data thieves have an arsenal of high-tech and low-tech ways to steal personal information. Once they have your information, they will be able to assume—and misuse—the identity of your customers. They may even try to assume your identity.

How Identity Thieves Strike

Low-Tech Methods

Dumpster Diving: thieves steal mail or papers with personal information left in the trash of your business or someone's home and not properly destroyed or shredded.

Mailbox Theft: thieves steal mail left in your business' unsecured mailbox or at someone's home.

Employee Theft: thieves within your business steal the personal information of your customers or of fellow employees.

General Theft: thieves steal an individual's wallet, check, credit/debit card with personal information, desk top and lap top computers—crimes often carried out by friends, relatives, in-home workers or others known by the victim.

High-Tech Methods

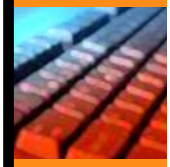
Computer Hacking: hackers get unauthorized access to your business computer or computer network and steal customer information from your database.

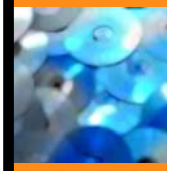
Phishing: thieves send fraudulent e-mails that appear to be from a legitimate company, and create a fake web site that looks like the legitimate company site. They do this to trick your customers into revealing their personal information.

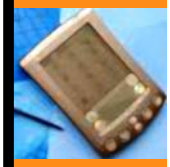
Pretexting: thieves make phone calls to your business and others in a "victim's" name, in an attempt to find out more information about the "victim." Or, they will call a consumer claiming to be from a legitimate company, and attempt to obtain personal information.

Real Data Theft Examples

- *An old laptop, with a company's customer records still on it, was sold via a newspaper ad. The records were still openly readable and could have been used to commit fraud by the purchaser, who alerted the seller about what he'd found.*
- *Two computers were stolen from a medical practice's unlocked computer room. They contained easily accessible billing records and unencrypted sensitive personal information in the form of billing codes.*
- *A courier service driver, carrying a package of customer data, left his unlocked vehicle running while he made another delivery. While he was away from his vehicle, the package was stolen.*
- *Perfectly readable, discarded printouts of personal records were thrown into a dumpster. They were later put to practical use by the finder to wrap fish at an outdoor market.*
- *In Florida, print-outs of thousands of medical records were found in various trash bins across the area. The records included details of sexually-transmitted diseases, psychological problems, addictions, and even intimate details about a patient's sex life.*
- *An employee in an accountant's office used client data to file false income tax returns in order to receive tax refunds ... until that employee was finally caught.*







What ID Thieves Want—Your Customers' Personal Information

Criminals are after credit/debit card numbers, Social Security numbers, driver's license information and numbers, mailing addresses, e-mail addresses, and telephone numbers. They also look for this information in your product orders, account statements and mail.

How They Use This Information

Data thieves will open fraudulent credit card accounts in your customers' names, make purchases without their knowledge, get a loan in your customers' name, or open a fraudulent bank account in your customers' name and write checks on that account. In addition, they can open fraudulent accounts with your business and make fraudulent charges to your customers' accounts…with you.

Small Businesses Can Be ID Theft Victims, Too

Business identity theft occurs when someone steals information about a business to commit fraud. Thieves may specifically target small and medium sized businesses because their data security programs may not be as strong as those of larger companies.

They want your business credit/debit card account numbers, your bank account numbers, your Federal Employer Identification Number, and other federal and state governmental identification numbers.

How They Use This Information

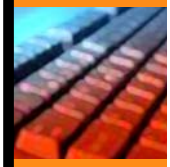
ID thieves can use your stolen business information to open a credit card account in your business' name, make purchases without your knowledge or get a loan in the name of your business. They will open a bank account in the name of your business, write checks on that account, and take out money from the existing accounts of your business. In some cases, ID thieves may secure enough information that they can actually sell your business or commercial property without your knowledge.

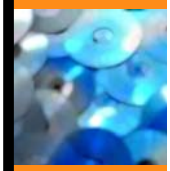
What You Can Do

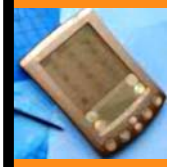
Here is a checklist of things you can do to protect your business from identity theft. You will find more details in Chapters 7, 8, 9, and 11.

Physical Security Tips To Protect Your Business & Your Customers

- Shred or cross-shred papers with personally-identifiable customer or business data before throwing them away, or use a document disposal company to destroy the papers for you.
- Send and receive business mail from a secured mailbox or a post office box.
- Conduct regular software audits of computers.
- Train employees to watch for suspicious activity among other employees, customers, or people coming to your business premises.
- Consider telling your customers how they can spot phishing efforts, and how they should verify that it's your communication before releasing any personal information
- Verify the identity of a customer before discussing or providing any customer account information by telephone or e-mail. Then take appropriate steps to provide it in a manner that is secure.
- Secure your physical space with locks and alarms.
- Secure your business, customer and employee records in locked cabinets.







7. Guidelines for Good Employee Practices

Screen Your Employees

Identity theft can originate in the workplace. Exercising care to hire honest employees is one of the best ways to help secure your business and reduce the risk of identity theft or fraud to you or your customers.

Past behavior is widely considered to be the best predictor of future behavior, though it is not a perfect tool. Conducting background spot-checks can assist you in learning and assessing the character pattern of prospective employees (or of your current employees—if you did not use a background spot-check before hiring them). The type of background spot-check to use depends on the size and nature of your business. If you handle lots of sensitive personal information, especially financial or health information, you might want to consider a full criminal background check. But if your business does not handle much customer personal information, a credit report can give you a useful snapshot of an applicant.

Because background spot-checks, themselves, raise privacy issues, handle this carefully. If you see a "red flag" in a background spot-check, confirm the accuracy of the information with the source before making a hiring decision.

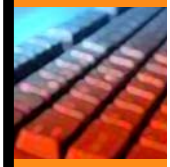
Other factors to consider in this process might include:

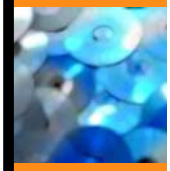
- Whenever you order a background check on a prospective or current employee, state and federal laws require that you notify the person (in writing) that you intend to use a consumer report, and obtain their consent to do it. This process is a key element of the federal *Fair Credit Reporting Act* (FCRA). Most background checks contain a "consumer report." If you decide to reject an

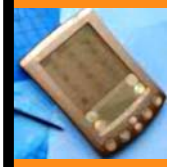
applicant or release a current employee based on something in their consumer report, you must tell them that you have done so for this reason.

- Many states have their own laws that apply to background checks and consumer credit reports. Discuss with your attorney the requirements in your business' home state or in other states in which your business makes hiring decisions.

Control Employee Access to Sensitive Data







- Each of your employees should have access only to the sensitive information necessary to do their specific jobs. *When you control employees' access to information, you significantly reduce the risk of data exposure.*

- You can limit employee access to customer information by using a variety of physical and technological security measures, ranging from padlocks to passwords. For specific suggestions, see Chapter 9, **Securing Data in Your Office and Online**.

Train Your Employees

Writing privacy and security policies for your business is not enough. Your employees need training for how to protect the privacy, confidentiality and security of personal information. Your training program should address all the issues discussed in your security and privacy policy.

Tips for Creating and Executing a Security & Privacy Training Program

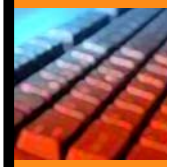
- Make it relevant, personal and timely.
- Tell employees why the topic is important to everyone involved.
- Role play with real-world scenarios that present examples of privacy and security choices your employees could face—and then explain how they should handle them.
- Have your employees sign a nondisclosure agreement, in which they will agree to keep your customer information confidential.
- Include your managers.
- Update employees on new developments in this area as they occur.
- Train employees to use computer security tools.
- Advise them on the dangers of purchasing or downloading pirated or counterfeit software.
- Train them to regularly update all security software and browsers.
- Train employees to spot phishing attempts, and not to respond to them. Keep them updated on new phishing ploys. For more information on phishing visit **http://pages.ebay.com/education/spooftutorial/index.html** or **http://office.microsoft.com/en-us/assistance/HA011400021033.aspx**.
- Use specialized training for employees whose job functions require it..
- Teach your employees how to look for suspicious activity from other employees, customers, visitors, strangers or acquaintances on your business premises.
- Train all new employees about your information security policies.
- Reinforce your employee training at least semi-annually to ensure that employees regularly put their training into practice.

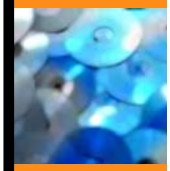
8. Collecting, Protecting & Disposing of Customer Data

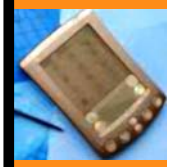
Collecting

The type of information you collect from your customers depends on your individual business, and can range from simply a customer's name, address, telephone number, and e-mail address to significantly more personal information, such as credit/debit card numbers, account numbers, transaction summaries, consumer preferences, consumer credit reports, etc.

If you collect and store credit card information, you need to follow security rules set by the major credit card companies. See Chapter 11, **Payment Card Security Requirements** for details **www.visa.com/cisp**.







If you don't absolutely need a piece of customer information, don't collect it. Collecting customer data you do not need increases your security and privacy risks.

Be particularly careful about collecting and storing financial and personally identifiable information, including Social Security numbers, credit and debit card numbers, or driver's license numbers. Check your payment transaction software systems to determine if it is collecting sensitive data you aren't even aware of, such as the magnetic stripe of a payment card or the PIN information from a debit card transaction. If you have customer data you no longer need, discard it—securely. See **Disposing** for tips.

Protecting

You need to guard against both high-tech and low-tech opportunists. If your business is not kept physically secure, anyone can walk in and steal unprotected customer data from your cabinets, drawers, and desks. This has happened. The same is true about your own employees if they have access to sensitive information they don't need or shouldn't have to do their job. One of the larger data breaches in 2006 stemmed from employee access to sensitive customer data that was inconsistent with their job description.

For tips on protecting against both high and low-tech predators, see Chapter 9**, Securing Data in Your Office & Online**.

Disposing

Disposing of personal data also is an access point for data/identity thieves. *Sloppy security practices in data disposal can lead to theft.*

The federal government issued a Disposal Rule amendment to the Fair Credit Reporting Act (FCRA), called the Fair and Accurate Credit Transactions Act (FACT Act). Both are enforced by the Federal Trade Commission. It mandates that all businesses that manage credit data—no matter their size—must take steps to ensure that discarded customer personal information is not accessible to unauthorized access. For more information on the Disposal Rule, and how it may affect your business visit: **www.ftc.gov/bp/conline/pubs/alerts/disposalalrt.htm**.

Currently, the law applies only to information your business gets from credit reports (or other "consumer reports"). However, it is good business to follow sound data disposal practices when discarding sensitive customer information, whether or not the law specifically requires it.

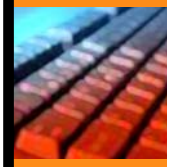
Disposing of an Old Computer

Before discarding an old computer, permanently erase all customer personal information on the hard drive. Deleting files by putting them in the "recycle bin" or "trash" on your computer's desktop is not good enough. These "deleted" files remain on the computer and can be accessed using commercial recovery software.

To ensure you properly "clean" an old computer, purchase commercial erasure software, available from most computer and office supply stores. This will overwrite all the data on the drive. You also can remove the hard drive and physically destroy it, so that it cannot be used again.

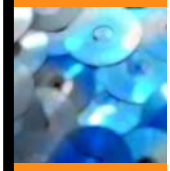
Disposing of Electronic Files (not on a computer)

If you are disposing of a computer disk, CD, DVD, or other electronic storage tool that contains sensitive information, the same rules apply. Don't just delete. Permanently erase the data, using commercial erasure software. Or, physically destroy the tool so that no one else can use it.

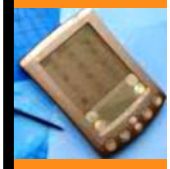


Disposing of Paper Files

Before throwing away any papers containing customer information, destroy the papers by shredding or cross-shredding, burning or pulverizing them.



If you don't want to do it yourself, hire a waste disposal company to shred or pulverize records for you. Articulate your requirements for disposal when using an outside company, and ask them to provide you with a quarterly report stating what they've disposed of, and how and when disposal was completed. If the company is local, you may want to visit their operations site for yourself and check their record with the Better Business Bureau.



9. Securing Data in Your Office & Online

The following guidelines generally apply to businesses that use a blend of hard copy and electronic methods to conduct their business activity, as most businesses do today. Remember that ID thieves operate using both high-tech and low-tech methods.

Physical Security

- Keep customer account records and other personal information in locked cabinets.
- Don't leave papers or files unattended on desktops.
- Never leave a business premise open and completely unattended, even for a short time.
- Use a locked mailbox or a post office box for incoming and outgoing mail.
- Use security envelopes for bills or other mail containing personal information.
- Shred anything with customer or employee personal information before discarding it.

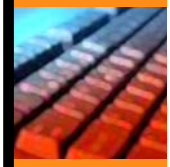
Computer and Network Security

- Use SSL technology for your online transactions. SSL stands for "Secure Sockets Layer," a technology that applies encryption —a scrambling of the message—to sensitive information traveling on the Internet, such as credit/debit card numbers. To use SSL, you will need to purchase an SSL Certificate from a Certificate Authority (CA). There are a number of Certificate Authorities you can buy SSL from, such as VeriSign **www.verisign.com**, Network Solutions **www.networksolutions.com**, Thawte **www.thawte.com** and GeoTrust **www.geotrust.com**. For more information on what encryption is and how to use it, visit HowStuffWorks **http://computer.howstuffworks.com/encryption.htm**.

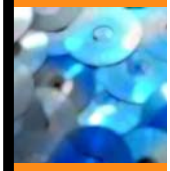
- Consider encrypting financial, medical and otherwise sensitive information on your on-site business computers. Your computer may already have the ability to encrypt data using settings installed on its operating system or networking hardware. Ask your

network administrator or computer vendor for assistance. If this is not an option, you can buy encryption software and hardware at most computer stores.

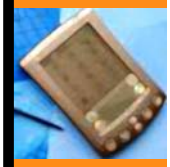
- Use passwords and change them frequently. Don't use a password that someone who knows even a little about you could guess, such as a spouse's or child's name, home telephone number, or college you went to. Never write your password down. The Federal Trade Commission provides helpful password tips at **www.onguardonline.gov/stopthinkclick.htm**.



- To the extent possible, don't keep personal information on the hard drive of computers that connect to the Internet. Use CDs, removable memory (flash drive), or floppy disks. Try to keep any disks or removable memory in a secure and locked location.



- Use a firewall to protect your computer network. Firewalls are a system of software, hardware, or both designed to prevent unauthorized access to a network. A variety of ready-to-use firewall programs are available from popular brands such as McAfee **www.mcafee.com**, Symantec **www.symantec.com**, and Zone Labs **www.zonelabs.com**. If your business handles especially sensitive personal information on the network and needs a higher level of protection, seek an IT consultant or visit a trustworthy computer store for suggestions.



- Continuously update your browsers, operating system, and other software to make sure you are using the most secure versions available. Updates can be found on the websites of the companies that manufacture the browsers, operating system and other software you use.

- Continuously update your anti-virus and anti-spyware software. Updates are generally available at the website of the manufacturer of the anti-virus and anti-spyware software you use. If you don't have anti-virus and anti-spyware software installed, contact an IT consultant or visit a computer or business supply store that you trust to find out what products will best fit your needs.

- Use file sharing only when you need it. Turn it off at all other times. You may want to consult a networking professional for expert security advice if especially sensitive information will be shared over a network.

- If you use wireless networking, turn on the security features that come with the wireless network products you purchase and test that they operate properly. Again, you may want to consult a networking professional before you share any sensitive information over a network. See **http://www.ftc.gov/bcp/online/pubs/online/wireless.htm**.

- Keep your network servers in a locked room.

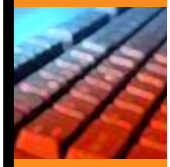
- Turn off your computers when not in use.

- Back up all your data regularly and keep backup disks or other back-up materials in a locked area.

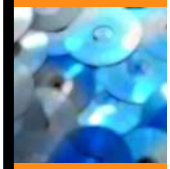
- Refer to Chapter 11, **Payment Card Security Requirements**. For more guidance, see **www.visa.com/cisp**.

Laptop Computer, PDA & Cell Phone Security

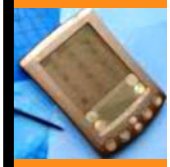
- Always keep your laptop, PDA, or cell phone within sight—especially when you are away from your office.
- Always keep your portable device within reach when traveling; stealing laptops at airports and from trains and restaurants has become a popular data theft technique.
- Limit the amount of any sensitive information stored on laptops, PDA's, and cell phones. If possible, do not store sensitive data on portable devices.



- Password-protect access to the laptop, PDA, and cell phone. Also password-protect features such as Internet access, e-mail, voicemail, and address books.



- Turn these devices off when not in use.
- Do not share portable communication/ organization tools (or their passwords) with others.



- If an employee (a salesperson or telecommuter, for example) needs to take personal data off premises on a laptop, CD, flash drive or other portable device, you should encrypt the data.
- Back up all data regularly and keep backup disks or other back-up materials in a locked area.

Special Protections for Cell Phone Users

Today's digital cell phones feature e-mail and Internet capabilities, address book and calendar functions, and can store recorded memos, voicemail, pictures, and other data files.

Although these features help businesses be more efficient, they also create a new layer of data security and privacy to protect. Criminals can hack into cell phones and steal stored files, contacts and voicemail. Viruses can significantly disrupt a cell phone, just as they do a computer. This is why it is important to lock your device and keep it in a secure location when not in use. Do not download or accept file downloads from unknown sources.

Limit the amount of data you transmit or store on a cell phone or PDA. Never store sensitive information, such as bank account numbers, ATM codes, and credit/debit card information on cell phones.

Cellular technology changes rapidly, and cell phone capabilities and security features vary significantly between models. Refer to your owner's manual for help to configure the security setting on your phone, or contact your cellular provider for assistance.

10. Internet Security Fundamentals

If you have an "e-business" or your business regularly executes transactions over the Internet, your security toolkit should include web site security, e-mail security, and advanced cyber-security tools.

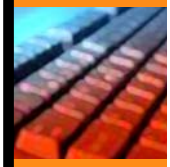
Web Site Security

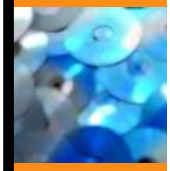
Customers have come to expect security on your business web site. Given this, you must ensure that you securely transmit all data over the Internet during an online purchase from your website. Secure Sockets Layer (SSL) is the industry standard for secure, encrypted data transfer over the Internet. SSL technology is built into all major Web browsers (e.g., Explorer and Netscape). Ask your web site designer to

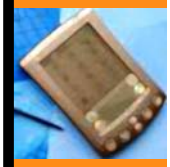
configure your site to accept SSL transactions, and ask for advice on how to get your SSL certificate.

SSL is a good starting point, but website security does not end there. Hackers also can steal stored information directly from computers, even if the information is not being transmitted over the Internet. As a result, go the extra step and consider encrypting any sensitive information stored on all your computers.

Refer to Chapter 9, **Securing Data in Your Office & Online** for information and links on SSL and data encryption.







E-mail Security

E-mail is not secure. Criminals can easily intercept e-mail transmitted over the Internet, and your employees, co-workers, or family members at home may have the ability to access your e-mail without you ever noticing. It's important to engage safeguards when you use e-mail.

E-mail Security Tips

- Use e-mail filtering software to screen e-mail and identify suspect messages.
- Don't open e-mail attachments or links from anyone you don't know or trust.
- Turn off the "preview" function of your e-mail program. While this allows you to see the first few lines of the email content, it can be a security risk.

continued

continued

- As a general rule, do not include sensitive information in unencrypted e-mail (Social Security Numbers, credit/debit numbers, account numbers, personal address, phone or e-mail information, etc.).
- When e-mailing messages to a group of people, put recipient addresses only in the "BCC" header (blind carbon copy)—not in the "To" or "CC" headers. This is important even if there is no sensitive content in the body of the e-mail; otherwise you expose the e-mail ID of everyone on your distribution list.
- Beware of "phishing." These are e-mails that mimic the designs of well-known sites and ask you to respond by giving personal information. Do not respond in any way to these e-mails. If you think the e-mail is genuine, directly contact the real organization and verify the authenticity of the e-mail. *Legitimate companies do not ask for personal information in an e-mail.*

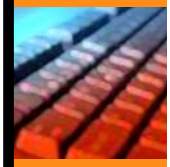
Cyber-Security Tools - The Basics

Using the right cyber-security tools can help you diminish the risk of data exposure from data handling.

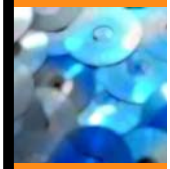
Here are the most widely used computer security tools and a brief explanation of what they do.

- *Firewalls*: software and hardware that limit external access to your business computers or network.

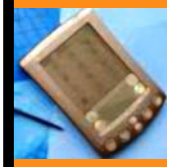
- *Encryption:* software or other technology that scrambles data to prevent unauthorized viewing.
- *Vulnerability Analyzers*: software that performs checks to determine if a computer network's devices and software are properly configured, patched, and updated.
- *Host/Network-Based Intrusion Detection Systems:* software that scans for network-related suspicious activity.
- *Intrusion Prevention Systems:* sensors that detect network security vulnerabilities.



- *File Integrity Systems:* systems that provide intrusion detection and verify that files have not been tampered with.



- *Network Scanners:* tools that identify network security holes that could give intruders access to your network.



These tools are available commercially at most computer or business supply stores. Ask your computer vendor, a sales specialist at a trusted computer store, your network administrator, or an IT consultant for the specific brand and product recommendations that will best match your system and your business needs.

11. Payment Card Security Requirements

Security Rules Your Business Must Follow

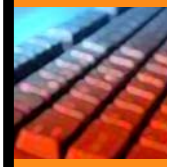
The major credit card associations (Visa, MasterCard, American Express, and Discover) have established security requirements for both credit card processors and merchants accepting payment cards. The following rules are especially applicable for your business.

- Do not store the contents of any credit card's magnetic stripe.
- Do not store the CVV or CVV2 (card verification value), two security features of debit and credit cards that should never be stored by businesses. The CVV is a secret code embedded in the magnetic stripe of payment cards that is used to prevent counterfeiting. The CVV2 is the three or four number code on the signature panel of most cards or the front of an American Express card.
- Store only the account information you need to complete and service your transaction. Under no circumstances should the CVV, CVV2 or PIN be stored.
- If you store the basic 16-digit credit or debit card account number, have a plan to destroy it when it's no longer needed. You may want to establish a policy that specifies the length of time your business holds on to credit card information.
- Ensure your business partners and vendors follow the payment card security requirements. A complete list of PCI compliant service providers is available at **www.visa.com/cisp**.
- Additionally, be aware of the unintended consequences of any software you are using. Merchants are encouraged to use point-of-sale payment software that has been validated compliant with the Payment Application Best Practices (PABP). A list of software providers/software applications that have been validated by PABP is available at **www.visa.com/cisp**.

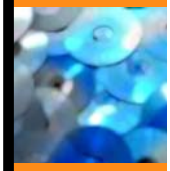
- Your business may have to comply with security audits according to the PCI requirements. You may be asked for a system's scan or self-assessment. Contact the bank or the company that manages your payment card processing for details or log on to **www.visa.com/cisp** for more details on the Payment Card Industry Data Security Requirements.

Security Rules for Processors—Which Also Apply to Small Businesses

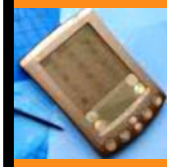
In addition to the guidelines listed above, payment card processors and merchants are required to follow these rules:



- Use firewalls.



- Change passwords and security codes from those supplied originally by the software manufacturer, to secure the processor's data and computer network.



- Encrypt all payment card information stored on the processor's computers.
- Encrypt any card data transmitted over the Internet or other public network.
- Use anti-virus software and keep it updated.
- Keep other software, such as operating systems, secure and updated.
- Provide employee access to data on a need-to-know basis only.
- Give each company employee who uses a computer a unique ID.
- Restrict physical access to hard-copy payment card data.
- Your business may have to comply with · Track card data access on the company's computer network.
- Test the company's security systems on a regular basis.
- Have an information security policy that spells out rules for employees who handle data and reinforce it regularly.
- For a full listing of these rules, go to **www.visa.com/cisp**. Click "PCI Data Security Standard."

By following the payment card security requirements, you will protect your customers' sensitive data, and put your business at a competitive advantage with other businesses that are not in compliance.

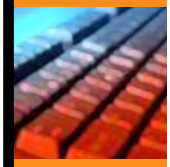
The alternative can be disastrous. If your business has a security breach and is found not in compliance with the payment card security rules, there are severe penalties, including barring your business from accepting payment cards.

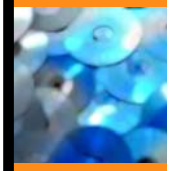
Choosing a Payment Card Processing Company

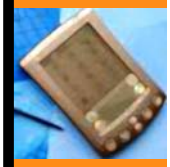
As a business, you have a choice in processors, and credit/debit card processors can vary in their performance. If your customers' information is lost or stolen from your card processor, you and your business could become the target of negative publicity, loss of customer trust, fines, and costly lawsuits.

As you select a processor, verify that they follow all the security rules required by the major payment card associations. If a credit/debit card processor fails to follow those rules, a major data security breach is possible. In 2005, hackers accessed information on approximately 40 million cardholder accounts from a credit card processor that was found not to be compliant with the credit card security requirements.

12. If You Have Data Lost or Stolen







Consider Notifying Your Customers

Currently, twenty-three states (listed here) have laws that require customer notification in the event personal data is lost, stolen, or inadvertently disclosed, and these laws may expand to a national level soon. Many states require you to notify your customers of *any* data breach. Other states require notification when harm to potential victims is likely.

Even if the law doesn't require it, consider the advantages of giving notice to your customers whose information was compromised.

If you tell your customers about the breach:

- Describe the nature of the incident.
- Tell them what you have done to address the problem.
- Tell them what you will do in the future to further reduce the chance of it happening again.

Notify Law Enforcement and Other Authorities

If a breach occurs, it is important to alert appropriate law enforcement officials immediately so they can investigate the incident. Talk to a lawyer to get advice on which law enforcement authorities you should contact. This could include local police, state authorities, or even the FBI. The major payment companies also advise that you immediately contact your payment processor and your acquiring bank if you have a credit/debit card security breach.

It is also recommended that if you have any kind of customer data breach, you alert the three national consumer reporting agencies: Equifax **www.equifax.com**, TransUnion **www.transunion.com**, and Experian **www.experian.com**. Visit the FTC Web site (**www.ftc.gov**) for more information on responding to a data breach.

Also alert the bank or company that you hire to process your payment cards. It's important that the compromised accounts are watched or

States with Breach Notification Laws

*Arkansas	*Louisiana	North Dakota
California	Maine	*Ohio
*Connecticut	Minnesota	Pennsylvania
*Delaware	*Montana	*Rhode Island
*Florida	Nevada	Tennessee
Georgia	*New Jersey	Texas
Illinois	New York	*Washington
Indiana	*North Carolina	

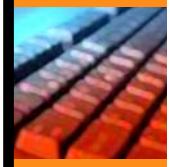
* Requires notification only when there is risk of harm to consumer victims

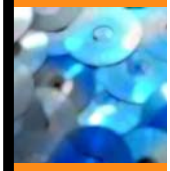
closed to prevent fraud from occurring on them. You could have liability for the resulting fraud, so quick notification to the payment card companies can help.

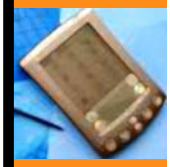
Ask your lawyer about this now, so that in the event something does happen, you are immediately prepared and know which law enforcement agencies to contact. Some local law enforcement departments have even set up special units to investigate such incidents.

Support Your Customers

If a breach occurs:







- Encourage your customers to monitor their credit reports for signs of identity theft. If you can afford the expense, consider paying for a credit monitoring service for your affected customers for a designated period of time (generally 6-12 months).

- Encourage any customer experiencing or suspecting identity theft to notify you, file a police report, and notify the three national consumer reporting agencies, outlined in the section on the previous page.

Responding quickly to a data breach may help you retain your customers.

13. Managing Official Requests For Your Data

You Have Both Duties and Rights

When you receive a request for customer records from a law enforcement officer or a government agency, balance your general inclination to respond immediately with your responsibility as a trustee of your customers' information.

Responding to Government Agency or Law Enforcement Requests for Data

- State your company's policies on responding to these requests in your security and privacy policy. If your business shares customer personal information with the government when it is required to do so by law or valid access request—say so.

- Consult with your attorney about your obligations to respond to government information requests and to ensure that you are complying with your privacy policy.

- Train your employees. Tell them what to do when they receive a request for customer information from law enforcement or other government agency.

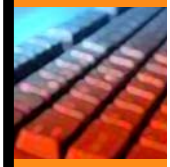
14. If You Do Business Globally

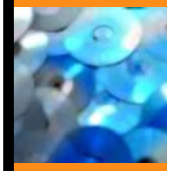
You Could Be Subject to Foreign Data Protection Laws

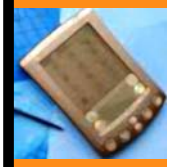
Over 50 nations have personal data protection laws that regulate the handling of consumer information by businesses. Most data protection laws apply to all businesses that handle customer information, regardless of size. Even a company with no physical presence in another country—but which engages in international business-to-consumer e-commerce—is often required to comply with these laws. These data protection laws are found throughout Europe, Canada, South America, Asia, Africa, and the Middle East.

What You Need To Know About Global Commerce

- Learn about the data protection laws in countries in which you do business. A good place to start is with the web sites of national data protection authorities for each country. Some publish guides to their laws that are customized for small businesses, such as the UK and Australia. For a list of data protection authorities in countries around the globe visit **http://www.dataprotection.ie/docs/European_Functions-Useful_Links/99.htm**
- Consumers in these countries expect businesses to understand and comply with local data protection laws, no matter what the business size.







What These Laws Require from Businesses

In general, data protection laws:

- Provide information to consumers about the collection and processing of their data.
- Process consumer data in a fair and lawful manner, and only for the purposes communicated to the consumer.
- Restrict the collection and processing of certain "sensitive" types of consumer data.
- Collect only relevant (and not excessive amounts of) personal data from consumers.
- Take reasonable steps to protect consumer data from accidental loss, destruction or unauthorized disclosure. This includes supervising employees and contractors who touch consumer data on a business' behalf.
- Ensure that safeguards are in place at destination points before transferring consumer information outside of the country.
- Check on whether a country requires businesses to file a notification with the national data protection authority before collecting and handling any consumer data.

Customers Have Rights Under International Data Protection Laws

Customer rights under data protection laws generally include:

- The right to withdraw consent to certain uses of personal data (generally for direct marketing uses).
- The right to obtain information about how personal data is processed.
- The right to view their personal information and request that any errors in that information be corrected.
- The right to sue a business in court for compensation or damages resulting from harm caused by a breach of the data protection laws.

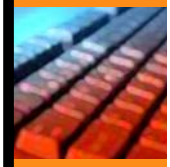
Law Enforcement

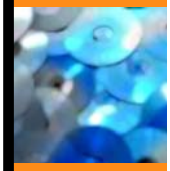
Most countries with data protection laws have designated a separate data protection authority to supervise and enforce the law. These agencies generally have the power to receive and investigate complaints about businesses from consumers, or to initiate their own investigations. Some have the power to impose fines and other penalties for violations of the law, while others may only make non-binding determinations (which may be enforceable by a court).

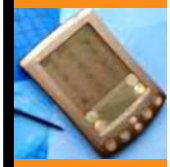
15. Additional Resources

Managing security and privacy in your business activities doesn't need to be an unduly expensive or time-consuming activity. Taking practical steps to protect the sensitive data your customers entrust to you will produce many dividends in return. Establishing solid data security and privacy policies and practices will:

- Put your business in compliance with federal and state law.
- Help protect your business and customers from data theft and criminal activity, including ID theft.
- Create a bond of respect and trust between your business and your customers.







Customers expect their information to be kept securely. Consider this your initial Guide to security and privacy best practices. However, note that security has new manifestations all the time, so it's a changing landscape. Here are additional resources to help keep you current.

- *The Better Business Bureau:* Find updates for small business owners about changes in security and privacy laws as well as new risks they need to manage. **www.bbb.org/securityandprivacy**.
- *The Federal Trade Commission:* The site of the nation's consumer protection agency has a collection of resources for businesses and consumers **www.ftc.gov**. The FTC also provides a one-stop national resource on ID Theft at **www.consumer.gov/idtheft**.
- *Privacy Manager's Resource Center:* a comprehensive resource from BBB*OnLine* to help businesses promote trust in consumer relationships **www.bbbonline.org/UnderstandingPrivacy/PMRC**.
- *IBM's Small Business Center:* a collection of resources for small business owners including white papers, technology solutions and expert Q&A **www.ibm.com/businesscenter/smallbusiness**.
- *Visa:* Full briefing of payment card industry (PCI) standards for merchants **www.visa.com/cisp**.
- *Business for Social Responsibility:* Issue Brief—Consumer and Employee Privacy **www.bsr.org**.
- *OnGuard Online:* provides practical tips from the federal government and the technology industry to help you be on guard against Internet fraud, secure your computer, and protect your personal information. Managed by the FTC **www.onguard online.gov/index.html**.
- *Small Business Computing.com:* an online magazine-style guide by Jupiter Media Corporation for small business owners featuring technology articles, reviews, and a message board **www.smallbusinesscomputing.com**.
- *Security Protection - Your Security Toolbox*: a site by Hewlett-Packard with links to a variety of information and tools for small business data protection **www.hp.com/sbso/security/toolbox.html**.
- *Microsoft's Small Business Center:* tips, tutorials, small business forum and product information for small businesses **www.microsoft.com/smallbusiness/hub.mspx**.