

SECURITY MATTERS:

Steps to safeguard your business

PRESENTED BY



TABLE OF CONTENTS

Introduction	3
How a Security Breach Impacts Your Business	3
Recognizing and Preventing Security Threats	3
Legal Responsibilities Affecting Every Business	4
Best Practices for Developing a Document Management Policy	6
Getting Started: Document Retention	7
Dispose of Documents Safely and Securely	7
Backup Solutions for Sensitive Information	8
Running a Responsible Business	9

ABOUT Fellowes...

Headquartered in Itasca, Illinois, Fellowes Inc. offers an impressive range of products to equip the work space, including paper shredders, binders and laminators, desktop accessories, and record storage solutions. Fellowes Inc. owns and operates subsidiaries in Canada, the United Kingdom, Benelux, France, Germany, Italy, Poland, Spain, Russia, Singapore, Japan, Korea, China and Australia. The company employs more than 2,700 people throughout the world and expects global sales in excess of \$700 million this year. For more information, visit fellowes.com.

©2008 Entrepreneur Media Inc. All rights reserved.

INTRODUCTION

Proprietary business information is your company's most valuable asset. Keeping it secure from identity thieves, disgruntled employees and other security risks should be a top priority for every business. This report clarifies the leading threats every business must know about, provides a detailed look at the state and federal laws governing how sensitive information must be handled both before and after a security breach, and offers essential steps every business owner must take to stay protected.

How a Security Breach Impacts Your Business

The costs of a security breach come in many guises. Equipment like stolen or lost laptops or phones may need to be replaced. Customer notification takes time and money, and you may need to offer—and pay for—credit monitoring services. A breach pulls your company's focus away from your core work and requires you to shore up your security procedures or formulate and implement a completely new security plan.

Legal counsel may also be required after a breach has occurred. According to a 2007 study by research firm Ponemon Institute, 85 percent of companies have experienced a security breach, and 59 percent of those faced potential litigation. But perhaps most damaging of all is the blow to your reputation. According to the same study from the Ponemon Institute, 74 percent of breached companies reported a loss of customers.

In addition, the financial impact of a breach can be staggering. According to a 2007 study by Forrester Research, the cost of a data breach ranges from \$90 to \$305 per customer record, as well as lost employee productivity of \$20 to \$30 per customer record. The discovery, notification and response cost an additional \$50 per record. It's rare that a security breach results in just a single customer record becoming compromised. Think about how

many entries you have in your customer list and calculate the potential impact of that list falling into the wrong hands. A security breach affecting 10,000 customer records, for instance, could cost your business between \$1.1 million and \$3.4 million, not including discovery, notification and response costs.

Recognizing and Preventing Security Threats

Effectively protecting your business means understanding which threats are most likely to compromise your security. The most common types of breaches come from a variety of sources:

■ **IDENTITY THIEVES:** According to the FBI, identity theft cost businesses and individuals \$56.6 billion in 2005. Identity thieves look to obtain information such as names, addresses, social security numbers, credit card numbers and bank account numbers. Identity theft can happen the old-fashioned way through dumpster diving or by more high-tech means. Identity thieves often target growing businesses, which sometimes lack the security measures large corporations have put in place.

Research shows that customers are concerned about issues like identity theft. A Zogby Interactive poll taken in 2007 found that 91 percent of respondents are concerned that their identity might be stolen and used to make unauthorized purchases. And one-third of respondents said they are not confident businesses are taking the appropriate steps to safeguard their information. If you're able to assure your customers of your security plans and demonstrate their effectiveness, you can expect customer loyalty and trust in return.

■ **COMPETITORS:** Corporate espionage may seem like a problem that only affects large organizations, but it happens to small and midsize companies as well. Intellectual property, marketing plans and customer lists are some of the most vulnerable areas.

■ **EMPLOYEES:** When an unhappy employee quits or is fired, he might try to leave with your customers' proprietary information. Pre-hire background checks can raise red flags before an employee even starts working for you. It's an especially good idea for employees who handle proprietary or customer data. For highly sensitive information, keep computer logs of who accesses the data and when. You'll be able to track the history of an employee's access with employee monitoring software. For particularly sensitive positions, a noncompete agreement or confidentiality clause in an employee contract can give you a measure of protection.

Always discontinue an ex-employee's ability to access your computer systems and physical office space as soon as he leaves. That includes turning off his e-mail account and changing passwords promptly. If you already have a policy for properly securing sensitive papers, you won't have to worry when an employee quits or is fired.

■ **ON THE ROAD:** The mobile business lifestyle has become ubiquitous today, and laptops and smartphones are more popular than ever. However, the proliferation of small devices full of business information has led to an increase in security breaches involving these gadgets. Lowering your risk means minimizing the important information you put on company laptops and phones. If you use small, portable USB flash drives, establish a policy of only using drives with strong encryption and passwords. Lastly, when doing business in airports, hotels and conference centers, always protect your sensitive paper documents upon disposal by shredding proprietary information.

According to the Computer Security Institute's 2007 "Computer Crime and Security Survey," the theft of proprietary data from mobile devices cost \$2.3 million in losses, while the theft of customer data from mobile devices cost more than \$2.2 million in losses. Protecting your equipment means keeping it with you at all times. Be aware of your surroundings, as well as who might be looking over your shoulder when you're computing in an airport or at a wireless hot spot. Passwords, encryption and biometric

devices like fingerprint readers are affordable measures you can take to protect laptops. The upfront cost is minimal when compared to the cost of a security breach.

■ **OUTSOURCING:** A growing number of companies now outsource some of their business processes. If you use web applications or bring in contract workers on occasion, you need to know that your business information is secure when it's outside your walls or in the hands of temporary employees. When dealing with an outside company, check its privacy policy and its reputation. Make sure it has high-level security in place, especially if it's handling your customer records or financial data. When it comes to contractors or temporary workers, follow up on references. Don't allow them access to sensitive information unless it's absolutely necessary.

■ **SOCIAL ENGINEERING:** This method preys on our innate sense of trust in other people in order to extract valuable information. For example, an employee might receive a phone call from someone claiming to be part of the business's technology support staff. He'll mention how he's working on upgrading the computer network and that he needs to reset the employee's system password. The unsuspecting employee gives up his password to the friendly, professional-sounding person on the other end.

It can be difficult to guard against social engineering, but awareness can be a powerful preventative measure. Educate your employees on social engineering so they know to be alert to phone calls or visitors to the business. Social engineering is one of the most common—and most overlooked—causes of a security breach.

Legal Responsibilities Affecting Every Business

Managing sensitive information about customers, employees and others has become such a complex issue

that the government has stepped in to offer guidance. A variety of state and federal laws now mandate a company's actions both before and after a security breach has taken place.

■ **FACTA:** According to a 2005 survey by zTelligence, nearly 87 percent of businesses didn't recognize the term *FACTA*. The Fair and Accurate Credit Transactions Act went into full effect in 2005. FACTA is designed to help prevent identity theft by governing the way businesses store, handle and dispose of certain consumer information. This wide-ranging act affects businesses of nearly every size. Businesses that deal with lending, mortgages, rental properties, private investigations or debt collection should take extra heed of FACTA. If you work in these areas, you are likely already dealing with a considerable amount of private information that is specifically covered under FACTA.

FACTA covers the use of consumer reports and information derived from consumer reports. This can include data such as credit reports, credit scores, employment background checks, medical history, check writing history, insurance claims and residence history. This applies to electronic data as well as paper documents. Sometimes it can be difficult to determine if information you are using in the course of your business came from a consumer report at some point. If you are unsure if a certain document falls under this requirement, it's better to be safe and treat it as though it does.

FACTA doesn't directly specify requirements for disposal methods, but you do have to render the information unreadable. For hard drives, DVDs, CDs and other digital media, you can physically destroy the items or have the data on them thoroughly wiped out. For example, if you use tape backup, you can degauss the tapes to effectively remove the information. Hard drives will require proper data overwriting and erasing techniques. CDs and DVDs can be destroyed in most paper shredders, depending on the type of shredder.

Complying with FACTA is in your business's best interest. Businesses that fail to follow the FACTA requirements and are found to be responsible for a resulting case of identity theft leave themselves exposed to civil lawsuits. On top of that, businesses can be assessed federal fines of up to \$2,500 per violation and state fines of up to \$1,000 per violation.

■ **HIPAA:** HIPAA is designed to safeguard Protected Health Information, or PHI. PHI identifies an individual and is received or created by a health plan. If you sponsor a company health plan for your employees, then you need to be in compliance with HIPAA. The amount of work a business must do to be in compliance can vary with the amount of PHI it has access to.

Make sure you implement written policies and procedures that ensure the privacy of employee health information. Keep files locked up, use passwords and encryption for electronic records, and use a shredder for document disposal. Failure to comply can result in large fines and even criminal charges for knowing violations. Civil penalties are \$100 for each violation, going up to \$25,000 per person per year for each requirement that is violated. Criminal penalties for willfully violating HIPAA max out at \$250,000 in fines and up to 10 years in prison for obtaining personal health information with the intent to sell it or use it for malicious harm. Wrongful disclosure can result in up to \$50,000 in fines and one year in prison.

■ **GLBA:** The Gramm Leach Bliley Act deals with consumer financial information. The GLBA's Privacy of Consumer Financial Information Rule is one section to pay special attention to. In basic terms, it says businesses that are "significantly engaged" in "financial activities" need to comply with the GLBA. This includes companies involved with loans, debt collection and real estate settlement services. Protected information under this rule includes a consumer's "nonpublic personal information." For example, information given on a loan application would qualify. You must give all your customers a privacy

notice that describes your privacy policies and practices. It's your responsibility to protect consumer information if you fall under the umbrella of the GLBA.

■ **FCRA:** The Fair Credit Reporting Act deals with an employer's responsibility when using consumer reports to hire or evaluate employees. Businesses that use employee or potential employee credit reports must first notify the subject in writing that a report may be used. If you use a report as the basis for denying a job or promotion, you must give the person notices both before and after taking action and supply this person with a summary of his or her rights under the FCRA. Any reports you obtain are also subject to FACTA security and disposal requirements.

■ **COPPA:** The Children's Online Privacy Protection Act applies to any operator of a commercial website or online service that collects personal information on children under age 13. Even if you run a physical business with a commercial website, this still applies. Requirements include posting a privacy policy on the homepage, providing notice about the site's information collection practices to parents and obtaining parental consent before collecting personal information. Site providers also have to give parents a choice about whether information can be shared with third parties and the opportunity to delete the personal information. Businesses are required to maintain the confidentiality and security of the collected data, whether it's in electronic or paper form.

■ **FTC ACT:** Section 5 of the Federal Trade Commission Act is notable for businesses. In short, Section 5 prohibits unfair or deceptive practices and is particularly applicable to privacy policies. It is designed to ensure that businesses follow their stated policies when they're assuring consumers of privacy and security practices. The best way to stay compliant with this law is to craft a privacy and security policy and follow it. Update it as needed if your situation changes or if you implement new or different security methods.

■ **STATE LAWS:** Federal laws are just part of the picture when it comes to security compliance. Laws targeting identity theft are spreading across the nation. Arkansas, Illinois, Louisiana, Maine, Montana, New York, Ohio and Texas are just a few of the states that have some form of breach notification law on the books. These laws can vary from requiring that any data breach be reported to requiring notification only when there is a risk to the consumer. Keep track of new legislation in your state and be sure your business complies with existing laws.

Best Practices for Developing a Document Management Policy

It's imperative that every business evaluate its security plans and policies. This encompasses everything from the locks on the doors of your office to the anti-spyware software installed on individual computers. It involves you and your employees working together on a clear mission to build and maintain a secure office. A proactive approach is vital, particularly when it comes to paper documents that can easily be overlooked when you're focusing on digital security measures. Paper applications filled out by employees, e-mail attachments that have been printed out and even handwritten notes about your competition all require protection.

Handling all this information is a challenge for every business; that's why crafting a document management policy is such a necessity. Having a formal plan in place helps your company retain the files it needs and clear out the ones it doesn't. It can also prevent the confusion that arises from having multiple versions of a document. Documents are important business assets that need rules to deal with their classification, security and disposal. A diligently applied set of policies protects you both legally and ethically.

Use templates for common documents like time sheets, contracts, invoices and letters. Even if you have multiple

employees generating such documents, you'll be able to easily classify like records together. Require a date or time stamp to differentiate versions of a document and to help keep your files in correct order. Consistent filing practices for both electronic and paper documents make retrieval later a simple task. Keep a record of where files are located and if they are available in paper format, digital format or both.

Lastly, trace the life of the electronic- and paper-based data that you keep. Whether it originates from forms on your website or from handwritten records at your office, evaluate where along the line it could be vulnerable and take the necessary steps to safeguard it.

Employee training is key when it comes to implementing a successful document management policy. Maintain a written policy and educate your workers on what types of documents should be stored and which should be destroyed. A standardized policy applied across the board takes the guesswork out of the process. And when it comes time to purge your company, customer and employee records, you'll be able to do it thoroughly and in compliance with applicable state and federal laws.

Getting Started: Document Retention

A good first step is to establish guidelines for the retention of company records based on what makes sense for your business. There are some general guidelines to follow for certain types of information. The Fair Labor Standards Act, for example, requires that employers keep payroll records for at least three years. Financial and tax records should be kept until any possibility for an audit has passed; 10 years is reasonable. If you offer products with a lifetime warranty, keep your sales records indefinitely. Set up regular reviews to inventory and purge documents, both electronic and paper. A biannual or quarterly review is a good starting point for most businesses.

Next, take inventory of your proprietary information and data—from employee records and market research reports to legal communications and tax records. This information is the lifeblood of your business, and customers and employees trust you to keep it safe. That means taking steps to protect hard drives and websites and ensuring employees don't tape passwords to their monitors. Make sure critical information, such as the innovative designs for a new product, isn't left out in the open. Such security measures are often straightforward and relatively easy to maintain.

There are plenty of sensible alternatives to simply throwing documents in the trash, placing them with the recycling or letting them stack up on a desk. To safely store reports, files and other critical information on-site for a certain amount of time, keep files locked away in a secure location. When it comes time to clear out old files, pay special attention to any documents that have social security numbers, financial details or tax records. It's hard to know exactly which documents might be valuable to identity thieves, snoops or competitors; if you're not sure, shred it.

Dispose of Documents Safely and Securely

Once you have an overall security and document management policy in place, it's time to focus on how to dispose of documents and outdated CD and DVD data backups. Follow these guidelines to pick a shredder that's a good fit for your business's needs. Often, a combination of shredders is the best solution. Basic specifications to consider are the number of users, the level of security (to determine the cut style), the number of sheets that can be shredded at a time, how many sheets need to be shredded per day, what kinds of materials will be shredded and the capacity of the bin.

Before investing in a shredder, do some research to familiarize yourself with the different features available.

For instance, Fellowes recently introduced a 100 percent Jam Proof shredder that prevents overfeeds and time-consuming jams. Some shredders even contain an auto-oil feature that maximizes performance and extends the shredder's life by automatically coating the cutters with oil. For higher-level security needs, consider a cross-cut or microcut shredder. Cross-cut shredders shred documents into small particles of uniform length and size, while microcut shredders literally turn sheets of paper into particles that are smaller than a staple. These kinds of shredders may cost more than a basic strip-cut shredder, but if your business handles highly sensitive information, the extra investment offers an additional level of protection. The interactive Fellowes Shredder Advisor (fellowes.com/fellowes/site/shreddertools) is one source that can help you narrow down the options to find an appropriate shredder.

Deskside shredders are compact and affordable machines designed to handle the needs of a single person or a home office. Prices can range from about \$100 for a light-duty personal shredder for occasional use to \$500 for a shredder with more features and the ability to handle a bigger workload. You may choose to set up a deskside shredder in the cubicle or office of any employee who handles sensitive information that needs to be disposed of immediately and privately. Your document management policies may require several deskside shredders as well as a larger, commercial shredder, or perhaps a heavy-duty machine, which is ideal for offices of one to three users with moderate shredding needs.

Commercial shredders—which can cost up to a few thousand dollars depending on features—are designed to handle a higher volume of paper. These are ideal for departments, workgroups, offices and warehouses where multiple users need to shred documents or where there is a high volume of sensitive paper. Law offices, accounting firms and businesses in the financial and health industries are just some of the companies that may want to opt for a commercial shredder.

When it comes to commercial shredders, the number of users is important. Look for shredders that are built to perform without interruption for multiple users. Sheet capacity, speed, bin size and continuous duty run times ensure that the job is completed as quickly as possible. Also consider basket capacity and the availability of anti-jamming features. You don't want to waste valuable employee time by having to clear a jam or empty a waste basket too often.

To be sure, shredders are a must-have business machine for every office today. They not only support your company's security policy, but also make it easy for employees to do their jobs efficiently and comply with security policies. Customers, too, benefit from your investment in a shredder. They share their personal and financial information with your business assuming that you will protect it. When your document management policy includes the use of shredders, it reassures customers and clients, who are increasingly sensitive about issues of identity theft and credit card fraud. Shredding documents is the ultimate assurance that their information won't fall into the wrong hands.

Backup Solutions for Sensitive Information

Security breaches, hardware failures and natural disasters are all unexpected events, but you can still prepare for them. If your business were to face such a scenario, would you be able to pick up quickly from where you left off, with your customer records still accessible and your valuable business information within reach? For many businesses, the damage could be irreparable. That's a strong indication that you need to take some extra steps to handle whatever situation you may encounter.

In terms of backing up digital data, there are a variety of methods available to businesses. Options can be narrowed based on budget and your business' specific backup

needs. If you back up your data to CDs, DVDs or other removable media, don't leave them lying around the office. Any disaster that takes out your office computers could also impact your backup disks or tapes. Establish a policy that requires you to take them to a secure, off-site location. Avoid leaving them in a vehicle that could be broken into, and use encryption software for any sensitive information. The same policies apply to external hard drives. Just be sure you use your chosen backup method every day. If you have more intensive network or server needs, a technology consultant can help you make off-site backup arrangements.

Hard drives do die, and they rarely give warning. Online backup services can be an effective option for smaller operations or if you need to back up laptop files away from the main office. Your data is uploaded securely through your web connection and kept by the service provider for easy recovery if needed. This also gives you a measure of protection should a virus or other malware program infect your computer. Perform the same due diligence when choosing a backup service provider that you would with any potential outsourcing operation.

Web applications have become more powerful over the past few years. You have many options for moving mission-critical needs like CRM, e-mail marketing, document creation and project collaboration to the web. This offers the advantage that your data no longer resides solely on your office computers. A reputable service provider will keep redundant backups of your data. Don't hesitate to ask questions about the security, privacy and backup policies of your service providers. You need to feel comfortable when you entrust your valuable business data to an outside party.

Running a Responsible Business

When you protect your business information, you are also protecting your reputation and relationships with employees

and customers. In a competitive business environment, you need to do everything you can to differentiate yourself. Having a comprehensive security and document management policy gives you an advantage over the many businesses that neglect this important and pressing need. It shows customers you operate a responsible and ethical business that cares as strongly about their information as they do.

Once you've built security awareness into your business, you can spend less time worrying about where potential threats are coming from and more time focusing on your core business. There will always be a component of ongoing education to security as hackers and thieves devise new methods of stealing information. But if you prepare to be flexible, keep up on the latest security news, and revisit your document management and security policies on a regular basis, you'll be able to run a secure operation that is protected from both internal and external threats.