Why you MUST protect your customer data

If you think you're exempt from compliance with customer data security and privacy laws because you're a small business, think again. Businesses of all sizes are responsible for compliance with these regulations—and those that don't comply may face fines or lawsuits.

Who should be concerned about security and privacy?

Customer data is a key currency of today's information-based economy; so regardless of your industry, you probably collect, store and share information about your customers. This data may include Social Security numbers, driver's license numbers, mailing addresses, e-mail addresses, telephone numbers, credit card numbers and bank account numbers. If you use any of this type of information, you need to keep reading.

How data thieves strike

Data thieves use a number of low-tech and high-tech methods to access your data. Here are some of the more common ones.

Method	Description
Dumpster diving	Thieves steal papers with personal information left improperly discarded in your trash.
Mailbox theft	Thieves steal mail left in your unsecured mailbox.
Employee theft	Employees steal the personal information of your customers or other employees.
General theft	Thieves steal wallets, checks, credit cards, or computers.
Hacking	Thieves obtain unauthorized access to your computer network to steal customer information.
Phishing	Thieves try to trick your customers into revealing their personal information by sending e-mails that appear to be from your company and/or creating a fake web site that looks like yours.
Pretexting	Thieves make phone calls to your business in a customer's name in an attempt to learn more about the customer.

Once data thieves have the information they want, they use your customers' names to open fraudulent credit card accounts, make purchases without their knowledge, open fraudulent bank accounts, write checks on that account, or even get loans.

Security breaches could damage your business

The Federal Trade Commission (FTC) recently sued 12 companies it accused of having inadequate data security practices. Even if you don't face legal action, your good reputation could be significantly compromised by data security breaches. Security breaches can erode consumer trust and, ultimately, hurt your bottom line.

You can be a target, too

Identity thieves want your business information. In fact, they may target small and medium businesses because their data security programs may not be as strong as those of larger companies. They'll take your bank account and credit card numbers, Federal Employer Identification Number, and other federal and state governmental identification numbers. They'll use this information to open credit card accounts in your business name and make purchases without your knowledge, open bank accounts in your business name and write checks on that account, or get a loan in the name of your business. In some cases, they can actually sell your business or property without your knowledge.

Small businesses are MORE at risk than large businesses

Popular wisdom may hold that large businesses are most at risk for identity theft and fraud—but that's not the case. As we've already shown, data thieves are flexible: They operate using both high-tech and low-tech methods. As a result, security applies to every business that collects and stores customer information. Small businesses are a particularly attractive target because they often don't have the strong data security protections that large businesses do.

Compliance isn't a choice

Regardless of whether you think you're at risk for data theft, you're legally required to take proactive steps to prevent it—no matter how small your company is.

For example, all small businesses must comply with the Fair Credit Reporting Act (FCRA) when seeking to obtain consumer reports, such as credit reports and employment reports, about potential customers and employees.

Other requirements vary by business type. Small financial businesses, for example, must comply with the federal Gramm-Leach-Bliley (GLB) Privacy Rules and Safeguard Rules—and companies that need to comply include those that might not necessarily think of themselves as financial, such as automobile dealers, tax planners, and some travel agents. Small health care businesses must follow the privacy requirements of the federal Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and its data security requirements.

As a small business owner or manager, it's your responsibility to stay current on privacy and security laws affecting your customers—so establish good security and privacy practices now.

International policies could affect you

More than 50 countries have personal data protection laws that regulate the handling of customer information—and even companies with no physical presence abroad have to comply if they engage in international business-to-consumer e-commerce.

Firewalls are not enough

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.

Consider this scenario from the Better Business Bureau: You've equipped your computer with the latest network security software.

But 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 information on your computer. Your employee reads the credit card number to the caller. But the caller isn't really a customer; he's a criminal who found the name and address of one of your customers in the trash.

Indeed, in small and medium businesses, the greatest data security risk might not be technology, but the uneducated end user. Symantec's SMB Information Protection Survey, which was published in June 2010, reported that 42 percent of small and medium companies have lost proprietary or confidential information—and of the companies that lost data, 23 percent blamed insiders inadvertently losing data, while an additional 14 percent blamed broken business process.

The point: It's not just about good technology. Effective security and privacy policies and proper employee training are also essential.

Creating a security and privacy policy

A security and privacy policy tells your customers how you will treat their personal information. In essence, it explains how you will collect it, how you will use it, and how you will keep it secure.

Once you have a written policy that accurately describes your intended treatment of customer data, you'll want to communicate it to your customers. For example, you could distribute it on paper by posting it on asign in your office, giving customers a written copy when they complete a transaction with you, or mailing it as part of a promotional piece. Alternately, you could distribute it online by posting it on your web site, and if your customers have agreed to receive e-mail notices from you, send it to them via email.

Communicating your privacy policy to your customers will increase the trust they have in your business—because when they know that you plan to use their information carefully, they will be more likely to share it with you.

Resources to help you write a privacy policy

Need help writing an online privacy policy? Consider these two sources of assistance: the Better Business Bureau's Privacy Planner, available at www.privacyplanner.com, and the Direct Marketing Association privacy policy generator, available at www.the-dma.org/privacy/privacypolicygenerator.shtml.

Employee education is paramount

Employees who handle customer information should play a significant role in protecting that information: In its 2009 data breach report, Verizon Business found that insider errors were a factor in two-thirds of all breaches it investigated on behalf of clients.

Think about all the different ways your business collects, stores, and uses customer information. Now list who handles or has access to the information. Anyone who appears on your list should play a significant role in protecting sensitive information.

Conducting background checks can help you assess the character of prospective employees (or current employees, if you didn't do a background check before hiring them).

Next, employees should have access only to the information necessary to do their jobs. When you control employees' access to information, you significantly reduce the risk of data exposure.

Finally, employees with access to information also need to be properly trained to follow your security and privacy policies and practices.

Act quickly when a breach occurs

If a data security or privacy breach occurs, you'll want to alert appropriate law enforcement officials immediately so they can investigate the incident. This could include local police, state authorities, or even the FBI.

Additionally, you'll want to alert your credit card processor and your acquiring bank, as well as the three national consumer reporting agencies.

Also keep in mind that you may want to—or have to—alert your customers. Currently, 23 states 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.

Let us help

Is your business and internal IT staff up to the task of helping you prevent data theft? Perhaps not. Trend Micro's 2010 corporate end-user survey reported that 21 percent of small business employees say that their internal IT departments should do a better job at protecting them from potential risks associated with data-stealing malware.

You may shy away from security tools and practices because of the perceived cost, but you can prevent many threats easily. Technology available to help you avoid threats includes data-loss protection (DLP) systems and services that stop users from unintentionally disclosing information they should keep confidential, such as e-mail monitoring programs.

Because we invest in continuous training on the relevant technologies, as well as stay abreast of the business and policy issues we can help you review the available technology and come up with a comprehensive solution that fits your business. Contact us today for more information.

Bit by Bit Inc.

Mailing Address

115 West 29th St

4th Floor

New York, NY 10001

Phone: 212-691-8081

Email: info@bitxbit.com

Web: www.bitxbit.com