Maintaining Compliance

CASE STUDY

Why a restaurant took compliance off the back burner

SITUATION Not fully understanding issues of compliance has cost small businesses millions. Take, for example, Carla Yarbrough, of Spanky's Marshside restaurant in Brunswick, GA. In August of 2006, her Point-of-Sale (POS) system was hacked, the criminals stealing the magnetic strip data from customer credit and debit cards stored on Carla's hard drive. Worst of all, the breach continued undiscovered for seven months.

"I thought we were compliant because we had brand-new POS systems," Carla remembers. On top of that, she wasn't even aware that the system was storing that information. But by being more aware of PCI DSS compliance rules and asking questions of her POS vendor, Carla could have potentially avoided the entire breach, and the hefty fines that came with it.

RESULT Unfortunately, the incident has had to serve as an expensive lesson to the company, which paid a total of $110,000 over more than a year to fully resolve the issue. Carla's first step was a forensic audit to determine the source of the breach as well as other vulnerabilities. Then she updated both technology and processes to address those vulnerabilities to prevent security breaches from happening again.

Carla was one of the lucky ones. Many small businesses simply can't afford the fines and are forced to close down. But Carla says the lesson is to look at the cost of compliance as a business investment because "the damages [of a breach] far outweigh the cost of upgrading your system."

Photo source: Veer® stock photos.
Photo does not represent Ms. Carla Yarbrough, Spanky's Marshside, or any related associates or products.

CenturyLink™ Business

What is compliance?

Compliance is a broad term. Basically, it means that there are certain rules for doing business with which you must comply. Some of the more well-known areas of compliance are the Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA) and Sarbanes-Oxley Act. Big companies have VPs and entire departments to manage their compliance. You have…you. And us.

Who needs to think about compliance? Practically everybody.

Federal compliance laws and regulations extend to a broad range of business types, and while they're designed to protect investors, customers and patients (in the case of HIPAA), they also add another layer of complexity when making technology and process choices for your small business. That's why no matter what type of business you're in, it's important to have a basic understanding of the different areas of compliance.

Why worry about compliance?

With the sometimes high cost of becoming compliant, many small and midsized businesses are asking, "why do it?" One motivator is the possibility of hefty fines or worse. But the most important reason is to mitigate the risk to your business from things like internal and external security breaches, accidental data leaks and fraud.

Small merchants with on-site credit card processing who are hacked and have not put PCI standards in place can be fined $20 to $30 for each stolen card number (up to $500,000).

— E-Commerce Guide[1]

[1] "PCI Security: Small E-tailers Face Large Fines if Hacked," Kerry Watson, September 1, 2009. http://www.ecommerce-guide.com/article.php/3837101/PCI-Security-Small-E-tailers-Face-Large-Fines-if-Hacked.htm

A high-level look: the main areas of compliance

Here's a brief overview of the three main areas of compliance facing small and midsized businesses like yours.

Payment Card Industry Data Security Standard (PCI DSS)

Who it affects: Banks, payment processors, merchants and any business or service provider transmitting credit or debit transactions.

In a nutshell: The PCI standard requires banks, online merchants and Member Service Providers (MSPs) to protect credit cardholder information by adhering to a set of agreed upon security standards.

The PCI DSS is a multifaceted security standard that not only sets rules for protecting customer account data, it also establishes penalties should that data be compromised. Unfortunately, there is no off-the-shelf technology solution to ensure PCI compliance. It just comes down to the right systems and practices. And remember the cardinal rule: if you don't need it, don't store it. Don't even collect it.

CenturyLink™ Business

Health Insurance Portability and Accountability Act (HIPAA)

Who it affects: Health care providers, health care clearinghouses, health care plans and health plan organizations.[2]

In a nutshell: Establishes national privacy laws and regulations for safeguarding protected health information (PHI) processed and transmitted electronically.

As with PCI DSS, there is no off-the-shelf HIPAA compliance product, so ensuring compliance means establishing some best practices. Take a close look at your security such as your firewall, email and chat encryption and user access. Put procedures in place to identify and respond to security incidents, document your policies, standards and technology as much as possible and assign an individual to be responsible for coordinating it all.

Sarbanes-Oxley Act (SOX)

Who it affects: Publicly traded companies[3] (but all businesses should take note).

In a nutshell: SOX sets stringent financial reporting requirements for U.S. publicly traded companies.

SOX was enacted in response to the famous collapses of Enron, Tyco and others. This sweeping legislation is intended to increase investor confidence by helping to ensure that publicly traded companies maintain verifiably accurate financial records. And while the law doesn't apply to privately held businesses, many investors now use compliance as the benchmark for whether a company's financial reporting is sound.

[2] http://www.cms.gov/HIPAAGenInfo/Downloads/CoveredEntitycharts.pdf

[3] Public companies with market capitalization less than $75 million are currently exempt from SOX assessment.

Compliance Q&A

Q: Should I worry about Sarbanes-Oxley if my business isn't public?

A: It's a good idea. Although only publicly traded companies are bound by the legislation, many investors now won't consider investing in another business that isn't compliant. Also, if you're hoping for your private business to be acquired by a corporation, being able to demonstrate compliance could give you a leg up over more successful competitors who can't.

Q: I collect a large amount of data for my business, and ultimately I don't need most of it. How do I make sure I'm compliant in the handling of this data?

A: For sensitive data, if you don't need it, don't store it. Don't even collect it.

Q: When I send out patient information, do I still need to worry about HIPAA compliance?

A: You're still responsible for patient information when you send it out. So make sure vendors and partners are compliant.

Related guides:

Preventing security threats and stopping unwanted activities

Managing data storage

Protecting your data

For more detailed information about maintaining compliance, please refer to the accompanying white paper on this topic.

CenturyLink™ Business

Need more? We're with you.

Your community representative is always happy to help. You can count on them as a resource for compliance solutions to consider that fit your specific business needs, budget and level of expertise, as well as advice and resources on a range of small business technology issues.

Visit **http://centurylink.com/smb-resources** to contact your community representative, and learn more about how technology can boost your business. You'll find information sheets, videos, case studies and more.

Service not available in all areas. Contact CenturyLink for details.

CenturyLink™ Business