April 2010

Washington smartCEO

required reading for growing companies

the healthcare issue

oh brother!

A family business survival guide

straight talk

Stop confusing your customers

reform at what cost?

CEOs offer a better healthcare prescription

TIM MCGILL
CEO
Hargrove, Inc.

the best-laid plans

From national conferences to DC's headline events, Hargrove puts on the show

THE LEGAL EDGE

A new wave of data regulation threatens to pull your business under

data duties

Imagine this nightmare. You've spent countless hours, cash and creativity moving your business onto the internet. Traffic and sales are ramping up. Then a hacker steals your customers' credit card numbers and goes on a wild spending spree. Now you're buried under an avalanche of lawsuits and the Federal Trade Commission has started an investigation. This is no hypothetical. It's a regular headline.

Ask TJX Companies, Inc., the Framingham, MA-operator of Marshalls, HomeGoods and T.J. Maxx stores. In the 2000s, a hacker plundered TJX's customers' credit and debit card data. Consumers slammed TJX with class actions in 2007, accusing the company of failing to protect their data – and then failing to swiftly report the theft. Attorneys general from dozens of states piled on with their own lawsuit. The FTC began sharpening its knives – uh, rather, started its own investigation.

TJX settled the class actions in 2007 for well over $100 million. In 2009, TJX paid the attorneys general $9.75 million to end their case. Finally, TJX entered into a Consent Order with the FTC, promising to maintain a comprehensive security program – for 20 years. Ouch!

TJX's miseries aren't isolated: In 2005, data-thieves stole customer names, Social Security numbers and addresses from ChoicePoint, Inc. In 2006, ChoicePoint paid $10 million in fines and established a $5 million fund for affected consumers in the largest settlement of its kind at the time.

In 2007, Bank of America paid $14 million to settle a customer class action claiming privacy violations. The lawsuit alleged that BofA sold customers' Social Security numbers, account numbers and other personal data to telemarketers and direct-mail marketers for millions of dollars.

In one extreme case, 8.4 million consumer records were stolen from a check-authorizing company and sold to direct marketers in 2007. Not only was the company, Certegy Check Services, heavily penalized, but in 2008 a company employee was sentenced to almost five years in prison for the theft.

What does all of this mean for your business? Well, when you take on people's data, you also take on certain duties – everything from not selling info without customer permission to protecting data from hackers. The consequences of not living up to these duties can be staggering: fines, lawsuits, government oversight, damage to your brand, lost customers and a plunging company value.

WAVES OF REGULATION

The first data duties arose out of the wave of privacy laws that hit in the '80s. Congress started regulating cable television operators' use of subscriber data; websites' collection of information from children; motor vehicle departments' disclosure of driver data; the sale of credit reports; disclosure of school records; and more.

The Gramm-Leach-Bliley Act made banks adopt safeguards protecting financial information and required them to issue privacy policies. Customers even got the right to opt out of disclosure to third parties. Similarly, the Health Insurance Portability and Accountability Act upended the medical world, restricting disclosure of medical data. No longer could the receptionist at your doctor's office shout across the lobby and ask how your hemorrhoids were doing. (Personally, I was happy about that!)

Now another wave crests over corporate America. Virtually every state is enacting data protection laws and the FTC is unfurling a potent new rule.

A 2009 Massachusetts law regulates every business that maintains certain personal data about a Massachusetts resident. Requirements include user-authentication protocols, secure access controls, encryption, firewalls, appointing a security coordinator, employee training, risk assessments and enforcement measures.

Folks, that's just one state!

Other new state laws require companies

Jack Garson is the founder and a principal of the law firm Garson Claxton LLC in Bethesda, MD, and is also the author of *How to Build a Business and Sell It for Millions*. www.garsonlaw.com. Contact us at editorial@smartceo.com.

jack garson

to report data thefts; prohibit employers from collecting certain information about their employees; and limit use of genetic information to determine eligibility for insurance.

We're only just getting warmed up.

RED FLAGS

Congress had to get into the act. Responding to widespread identity theft, Congress enacted a law that spawned the "Red Flags Rule." This rule requires affected businesses to adopt an Identity Theft Protection Program. Generally, the rule applies to all businesses that lend money or extend credit by providing goods or services now and billing customers later. This includes banks, thrifts, mortgage lenders, utilities, telecommunications companies, health care companies, debt collectors and car dealers. (C'mon, haven't the car dealers had enough already?)

Under the program, you must:

- Identify the activities that signal possible identity theft for your business.
- Detect the warning signs of identity theft, such as change of address requests that often precede fraudulent spending sprees.
- Respond to potential identity theft, including contacting your customer or law enforcement and refusing to open a new account.

Many other requirements apply. In fact, because of the complexity, the FTC has delayed enforcement of the Red Flags Rule until June 1, 2010.

THE WORLD'S A-CHANGIN'

In today's world, any business that operates on the internet – or even just stores customer data – faces a barrage of threats and legal mandates. You need a security program designed for your business. A smart CEO should start here:

1. Create a data protection and compliance team.
2. Learn the legal requirements that apply to your business. Monitor new laws.
3. Consider lobbying to shape these laws to meet legitimate business and consumer needs.
4. Develop your compliance program. Communicate it to your employees and, as appropriate, your customers and vendors.
5. Implement your data protection program.
6. Monitor compliance with your program and record the results.

The world, it's a-changin'. We've replaced phone calls with emails, relationships with networks, judgment with algorithms. We store it all on servers and hope we're not sticking our chins out too far. But we're vulnerable to hackers and every conceivable fraud.

Fight back. Fight smart. CEO