



## Building a Safety Net

### Finding the Optimum Balance between Privacy and Profitability

By Mark Greisiger and Gary Clayton

Almost every day there is another story of a serious security breach. Indeed, over the last ten years, there seems to have been a dramatic increase in the incidents of security breaches and the loss and misuse of private customer information, credit card and other sensitive data. With each new incident, consumers grow more and more concerned about the privacy and security of their personal data. Unfortunately, from actual experience, the retail industry understands better than most that a loss of consumer confidence results in fewer sales, reduced profits and lower stock prices.

### Why the Increase in Breaches?

Are there really more security breaches today than a decade ago? Or are data breaches simply being reported today whereas a decade ago they were not disclosed?

The answers, like the problems, are not simple. Indeed, there probably are more security breaches today than a decade ago – if for no other reason than with the growth of information technology, businesses, schools, organizations and the government are all able to capture and use more personal information than ever before. As a result, personal data about customers, members and citizens is growing in value. And as data grows in value, the risks increase as well. Threats from hackers, thieves and employees make it imperative for businesses to implement safeguards.

### What's the worst that can happen?

Even the most privacy-focused company can be victimized by a data breach. When a breach event occurs, the consequences can be financially crippling. Recent studies have shown that the cost for data breaches ranges from \$180 to \$300 *per record*.

At least 39 states now require companies, by law, to notify every person whose sensitive personal identity information was compromised—which can take weeks and a huge expenditure of manpower. Systems may need to be shut down, business interrupted, and a public relations campaign launched. Computer forensic investigators and lawyers need to be hired. Information assets need to be restored. If the breach involved credit card information, cardholders, issuing banks, and credit bureaus need to be notified. Consumer banks might seek reimbursement for credit card-related losses while consumers may demand credit monitoring services. There may be class action lawsuits. Corporate officers may be held personally liable. If the breaches involve customers outside of the United States, penalties may include criminal sanctions against the business and/or against individuals.

### Don't panic!

Before you throw up your hands and walk away, there is good news: you're not expected to provide absolute security. The law recognizes that in today's networked world, it's not possible to require absolute security. What's required is that you provide safeguards that are appropriate to your company's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles.



## What safeguards are required?

The Federal Trade Commission (FTC) has played an active role in pursuing actions against companies that have failed to appropriately safeguard personal data. In the BJ's Wholesale case (File No. 042 3160), the FTC essentially created a national, non-statutory standard requiring all business that collect and maintain personal information to implement an effective information security program. The program must include a risk assessment that addresses the company's overall collection of personal information. The company must also make "reasonable" choices about how to mitigate the risks identified. Finally, it must regularly test, monitor and re-evaluate the program to ensure it keeps pace with developments in the information security field, as well as the operations and environment of the company.

New to retailers, in October 2007, federal financial institution regulatory agencies and the FTC issued new rules to the Fair and Accurate Credit Transactions Act (FACTA). Once exclusively focused on financial institutions, FACTA now requires any creditor that holds any consumer account, or other account for which there is a reasonably foreseeable risk of identity theft, to develop and implement an Identity Theft Prevention Program. The Board of Directors must sign off on the written plan, which makes them personally liable to the FTC. The new rules became effective on January 1, 2008, with compliance required by November 1, 2008. The new FACTA rules affect an estimated 11 million U.S. companies.

Lastly, for companies that process credit cards, the Payment Card Industry (PCI)'s Data Security Standard (DSS) has been established to help safeguard credit card information. The PCI DSS is a set of twelve requirements that are reasonably specific about what is required from a security standpoint. They're organized into six logically related control objectives:

- Build and maintain a secure network
- Protect cardholder data
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an information security policy

## Four Steps to Better Protection

So, what can you do to ensure that your daily business operations comply with your privacy and security policies as well as applicable laws and regulations? Here are four things you can do immediately to improve your security and privacy posture and reduce your overall risk.

### (1) Know your data.

The first step in protecting personal data is to determine whether or not the information is necessary to accomplish the business purposes for which it is being collected. Too often businesses collect personal information – Social Security numbers, birth dates, credit card numbers – even though they are not necessary to accomplish a business purpose. Your first step should be to ask if particular information is necessary. If it isn't, then don't collect the data. This obviates the risk. If, however, the data is necessary, you should document why it is necessary and how long it is needed. Once the information is no longer required for the identified business purpose, it should be destroyed.

### (2) Know yourself.

Obtain an independent, enterprise-wide network security assessment that evaluates the people, processes and technology underlying your security and privacy posture. An objective, third-party assessment allows you to identify specific vulnerabilities, so you can focus on hardening security



precisely where it's needed. In other words, it ensures that you spend your security budget on necessities, not luxuries. The assessment should include a third-party penetration test to evaluate whether internet-facing systems are capable of deflecting the known hacker exploits that threaten retailers.

**(3) Know your suppliers.**

You have an obligation to use suppliers and processors who are competent to adequately protect your company's personally identifiable information. This requires that you have a basic knowledge of the capabilities of your suppliers, how their personnel are trained and what processes and procedures they have in place to protect your data. Verify that the data is either returned or destroyed when it is no longer needed.

Make sure you have attorneys working with security professionals to interpret privacy and security laws and put policies and procedures in place that comply with those laws. Attorneys should also be engaged to address external contractual relationships with service providers, including drafting privacy and security contract terms to establish security controls, incident response, enforcement and monitoring, and transferring risk of loss.

**(4) Know your risks.**

No matter what measures you take or how much you spend on training, network security or physical safeguards, residual risk will always exist. Consider transferring the remaining risk through network and privacy liability coverage, now offered by several insurance companies. With this approach, you'll reduce your overall expense for network security and privacy protection. Remember however, while you may be able to transfer financial risks, you can't transfer the duty to implement and maintain appropriate safeguards.

**Conclusion**

No one wants to experience the embarrassment, hassle and expense of a data breach. Yet, it is likely that most of us will experience a breach incident despite our best efforts. Companies that have taken the appropriate measures beforehand will be able to minimize the damage. Only when you implement an ongoing program for data protection can your organization effectively walk the tightrope between privacy and profitability.



## About the Authors

### Mark Greisiger

Mark Greisiger is the president of NetDiligence<sup>®</sup>, a leading cybersecurity assessment services firm and a PCI Approved Scanning Vendor (ASV). NetDiligence's services are engaged by the majority of US & UK insurers in the privacy liability industry to evaluate their policyholders' networks. Mark is an authority on cybersecurity and network risk for computer-dependent businesses, government agencies and financial institutions. He is a member of Infragard, a partnership between the FBI and the private sector focused on cyber infrastructure protection, and a frequent author and speaker on network liability and cyber risk insurance. Mark can be contacted at [mark.greisiger@netdiligence.com](mailto:mark.greisiger@netdiligence.com).

### Gary Clayton

Gary Clayton is the founder and CEO of Privacy Compliance Group, Inc., a leading privacy and data protection consulting company. Privacy Compliance Group works with companies and government agencies to establish effective privacy compliance programs and to develop practices and policies to comply with privacy laws around the globe. Gary has worked with leading multinational companies and with numerous agencies of the US Government, including the Department of Homeland Security, the Department of Transportation, the General Accounting Office and the Federal Trade Commission. An attorney who is admitted to practice in Washington, D.C., Texas and Louisiana, Gary is a frequent author and speaker on global privacy and data protection issues. He can be contacted at [gclayton@privacycg.com](mailto:gclayton@privacycg.com).