



Protecting Customer Data:  
How Much is Your  
Customer's Trust Worth?  
Part I: The Business Case for Privacy

## Contents

The Two Sides of Customer Data: Business Necessity vs. Business Risk .....	3
A Company's Strategic Need for Data.....	3
What is Trust Worth?.....	5
The Unmet Consumer Data Protection Challenge	5
Privacy's Affect on Customer Confidence ....	5
A Potential Setback of Consumer Online Purchasing and Usage .....	6
When Consumers Lose, Businesses Lose Too	7
Why More Companies Aren't Taking Action .	7
Data Security: What Is Your Company Doing About It?	8
The ChoicePoint Crisis: The Tip of the Data Disaster Iceberg .....	8
FTC Study Reveals the Magnitude of Personal Identity Theft Crisis .....	9
Zero Liability Does NOT Mean Zero Damage	10
Conclusion .....	10
About The Authors.....	11
References.....	12
About Hitachi Consulting .....	13
About Hitachi .....	13

## The Two Sides of Customer Data: Business Necessity vs. Business Risk

Jane and her husband, both professionals living in Michigan, were looking forward to buying a third home. The first one was their residence, the second one a rental property. Having saved and scrimped, they were finally moving up in the world. They were shocked when their loan was denied. Unbeknownst to them, Jane's credit rating was a mess. After investigating, they discovered a person in Texas had used Jane's name and social security number to obtain numerous credit cards, a new BMW, and healthcare services. Could anything be worse than this? Yes. To top off the bad news, they also found that the thief had used their identity to get the deed to their second house and sell it.

Another gentleman, Mike, went to apply for a job. Not just any job, it was the opportunity of a lifetime he had worked toward for many years. As a retired Army Lt. Colonel, Mike had a distinguished service record and perfect credit. When the agency conducted a background check for this secret level clearance, they found something Mike could not believe. Someone had taken his identity and purchased three cars and other items worth over \$150,000 using his name. Despite a lifetime of integrity, he was essentially accused of theft and treated like a deadbeat. He had no idea identity theft could happen to him. Unfortunately, he lost the job as a result of it.

*Within the last six months, data privacy has literally become a household phrase for millions of consumers whose personal credit information is now in thieves' hands. And these thieves are doing more than just opening up fraudulent credit card accounts. They are after property and anything else they find personal information attached to. Who would have thought it would get to the point that identity thieves would begin using personal information to transfer the deeds of their victims' homes for quick sales to unsuspecting buyers?*

*The problem for consumers is that by the time lawful owners and duped buyers figure it out, the criminal is long gone. What problem, or problems, does personal identity theft pose for companies, if any? This topic is quickly becoming a huge strategic issue for companies; one that will cost them greatly if they don't understand the connection between personal identity theft and their bottom-line.*

## A Company's Strategic Need for Data

*Executives are bombarded with marketing messages about creating a single view of their customers, CRM analytics, business intelligence, and the use of data in marketing and sales. By combining customer-facing technologies with analytic techniques, such as collaborative filtering, predictive modeling, business rules, and customer intelligence, and historical data via predictive science, you can forecast future customer decision making about purchases. Data is required to shape how companies innovate products, how they go to market and which customers they focus on, and how they respond to customer inquiries in the contact center. Access to real-time, reliable and correct data is required for superior customer service, effective telesales and order management. In fact, obtaining and using customer data has never been more important to the strength and positioning of a company's success.*

*While executives are bombarded with marketing messages about collecting and using customer data to gain market share and increase revenue and profits, they are also reminded by reports from major news organizations, including CNN, MSNBC, and Fox on breaches of data security in corporations just like theirs. For instance, Citigroup recently reported the loss of personal information*

for nearly four million customers. A similar mishap at Bank of America led to the loss of consumer data, and Cal-Berkeley's recent victimization came in the form of the theft of a laptop from its admissions office. Lexis-Nexis, ChoicePoint, and others have also reported incidents of lost or stolen data. Even Paris Hilton's Sidekick was hijacked.

If you're listening to the stories reported in the news, you may be wondering why this is happening to so many companies. You might even be thinking it's probably a matter of when, not if, your company will be a victim.

"Within a company, customer trust equals value times security times privacy. Not all have to be equal, but if any of these three elements are zero, there's no trust. But how do you build trust? My recommendations include thinking holistically about your firm's strategies over the long term, inserting privacy considerations at every point possible. The consumer's point of view should be taken into account at all times."

—Peggy Eisenhauer, Attorney  
Hunton Williams

"The rational connection of brand, shareholder value and privacy is something we [privacy professionals] all get." Getting the rest of the organization to understand this idea and bake privacy into daily business processes becomes more challenging."

—Paul  
Cullen,  
Privacy  
Strategist  
Microsoft

With countless ways for a thief to steal identity, it is no longer surprising when the FTC says one in ten of Americans will become a victim of this crime. It begins with a thief gaining access to key pieces of data, which, unfortunately, is easier to obtain than people think. Everyday we write checks at the grocery store, purchase things online, make calls on cell phones, pay bills, order new checks, or apply for a loan or a new credit card. Most of us don't give these transactions much thought. We have become accustomed to sharing personal information from our income to our social security number, and of course our name, address and phone numbers.

Although there has been a somewhat unspoken agreement that people doing business will not steal other people's information, thieves do not abide by that agreement. They realized it was easier to steal information than to mug a person. The problem is that once a resourceful identity thief obtains our personal information, they can use it without our knowledge to commit fraud or theft, leaving us victims until we apply for loan or that dream job. It is at that moment the rude awakening occurs.

While the success of many companies is clearly dependent on customer data (information), individual privacy is recognized as a basic human right to be preserved (Warren & Brandeis, 1890). This right implies that individuals should be able to determine for themselves how and when their personal information is communicated to others. Customer privacy, based on this basic right, is concerned with how companies collect, use, and share Personally Identifiable Information (PII) and other sensitive data about their customers.

PII is generally defined as name, address, social security number, phone number, email address and triangulated data. Sensitive information includes an individual's financial, medical, credit, and political information. With the drive to collect and evaluate PII from customers, companies are facing new challenges that can and will negatively affect their financial success unless they have a framework to collect and protect consumer information.

Because many great companies are finding themselves in a situation that they never dreamed of, and because data is such an important business asset, we have written several whitepapers on this topic. The issues of data quality and creating a single view of the customer are addressed in other whitepapers. In this paper, we address the issue of customer data privacy and the financial implications to the consumer and the companies they purchase from.

The purpose of this whitepaper is to:

- Identify the current issues with customer data and identity theft
- Connect the impact of consumer identity theft to a company's ability to continue to collect and use customer data and
- Explain how customer data theft reduces customer trust and this can dry up contact center and online sales, affecting the company's revenue and profits

"My credit card company told me I was now a credit risk since my information was out there and they cancelled my perfectly paid platinum card without any notice. I was trying to use it at a store and the clerk told me it was cancelled. When I called the credit card company, even though their TV commercials said otherwise, they were nasty to me, blaming me for the ID Theft. Zero Liability, I don't think so..."

—ID Theft Victim

## What is Trust Worth?

If you need evidence that privacy has become much more than a legal issue, consider that for the first time in its five-year tenure, the annual International Association of Privacy Professionals (IAPP) conference included a strategy track on consumer data protection. The theme: Get privacy discussions out of the server room and legal library into everyday business. How to do this? When in doubt, bring up the bottom line. Research by CoreBrand, assessing the impact of a negative incident on brand equity and shareholder value, suggests that upwards of 10 percent of shareholder value can be tied to brand. If consumers' trust in a brand is compromised, business suffers and shareholder value slides.

Privacy needs to transition away from a single department compliance program to a corporate-wide business strategy, but the task to get those outside the "privacy bubble" on board is daunting. The key to getting the whole organization to understand the value of privacy initiatives is understanding how privacy ties into the corporate mission. It is also important to see how different internal stakeholders deal with privacy in each part of the business. Our research shows that an Organizational Change Management initiative is required to mitigate the internal politics and create buy-in and ownership throughout the entire enterprise. With an integrated view, a true corporate message about privacy can become part of everyday business.

## The Unmet Consumer Data Protection Challenge

Companies need to rise above the compliance issues around privacy and think about how to deliver on privacy strategy. Why? Because any change in the level of customer equity (the sum of all the lifetime values of a company's current and future customers) means the revenue and profits of a company are at stake. The value a company receives from each customer can be calculated with a Customer Lifetime Value (CLTV) equation. Maximizing the relationship with the customer means creating the most overall value possible for each customer. This is most likely to occur when customers most trust an organization to respect their interests. Obviously, privacy protection plays a big role in determining how much your customer will trust you.

For a company committed to its most valuable asset (customers), the data protection interests of the customer and the company can be aligned. If customers are a company's true source of value creation, then maintaining their trust is imperative. And, when companies understand this, privacy protection will become an important business tool, rather than just a regulatory requirement (which is how many companies view the task today).

## Privacy's Affect on Customer Confidence

Privacy has long been important to customers and studies show it is a factor limiting the acceptance and use of online commerce for 70 percent of online users. Several recent developments have heightened the awareness of this issue in the minds of consumers.

The first development is the alarming incidents of identity theft, which has affected upwards of thirty-three million U.S. consumers. The second is the rapid proliferation of "spyware", which tracks consumers' online activities for marketing and other purposes. In the financial services industry, privacy regulation has led to consumers receiving notices that describe the information being gathered about them and how that data is used and (often) sold to third parties. This regulation, part of the Gramm-Leach-Bliley Act of 1999, also asks consumers to make choices about their privacy. The highly publicized data losses by Choicepoint, NexisLexis and Bank of America has shown that technology infrastructures, in general, are not architected with privacy as a main business priority. In addition, there are limited audit trails and information about privacy preferences.

*"Privacy is not about the word, it's about doing what's right for customers."*

—Jennifer Barrett  
Chief privacy leader, Acxiom

But without adequate protection of customer data, sales and revenue goals are endangered. How? While credit card companies offer zero liability if a consumer's data is stolen, new research has shown that zero liability does not mean zero personal damage to the consumer. If more consumers understood the actual repercussions that identity theft can have on their life, a company's sales and revenue via the internet or the multi-channel call centers would dry up in an instant. Now *that* is something executives who are spending millions on CRM and contact center applications will want to direct attention to in the near future. If consumers lack the trust of organizations they bank with or purchase from, how many will be willing to take a chance to shop on the web or to disclose personal information to place orders over the phone?

With consumer identity theft on the rise, businesses are facing significant, new legal, financial, and public relations risks related to customer information privacy. If consumer confidence decreases, revenue could be diminished by brand degradation. Government legislation is often too slow to help businesses stop brand degradation or is ineffective in protecting consumer data, especially in today's fast-paced business environment. So, companies must begin creating, not only a corporate protection strategy, but also quickly implement practical methods to protect customer data to maintain and gain customers, especially for online purchases.

Because privacy is considered a basic human right in many parts of the world, it is vital in developing and maintaining trusted relationships. Forward-thinking organizations will move privacy up in strategic importance because privacy policies are a tool to improve customer satisfaction, trust in the company, and propensity to continue to do business with those firms. However, viewing privacy as more than just a compliance chore is an ideal not yet reached in many industries.

Our research shows that all companies strive to safeguard their customer information, using the highest standards of data protection, but they realize they don't know everything about the new found sophistication of the ID theft criminal world. Companies that assess their current state of data and learn how to protect their customers will increase the confidence of present and new customers. The question remaining is how do companies evaluate their current consumer data protection abilities, institute new policies and procedures, and communicate to consumers the changes they have made to protect their data and their lives?

## **A Potential Setback of Consumer Online Purchasing and Usage**

The banking industry is a prime example of growth resulting from e-commerce. Banking tends to be an industry where customers perceive very little difference between institutions.

Research conducted by Keynote Customer Experience (CE) with more than 2,000 customers of 10 leading online banks measured 250 metrics. CE's study found online banking capabilities are now more important to consumers than the number of physical locations or ATMs in determining where to open new accounts. The CE study found online bill payment customers are 20 percent more likely to purchase additional products and services from their bank and are 34 percent more likely to recommend their bank's website to others.

Forbes.com and ForeSee recently issued their second online banking survey, which showed a 5.5 percent increase in overall satisfaction with online banking. Customers who paid bills online were more satisfied than those who do not. This provides banks with an opportunity to increase satisfaction and loyalty by online bankers to online bill payers.

The Online Publishers Association (OPA) showed in its U.S. Marketing Spending Report of observed purchases by internet, that online users grew 8.3 percent

and the number of paid content purchasers increased 24.6 percent during the same period.

However, in light of increasing e-commerce statistics, according to the 2005 Privacy Trust Survey for Online Banking, 57 percent of respondents said they would immediately cease all online services with their current bank in the event of a single privacy breach. That would translate into millions of lost customers. With the growing wave of fraudulent “phishing” e-mails purporting to be from well-known banks, ISP providers and credit card companies, privacy and security issues are now undermining the progress web banking has achieved.

As a result of the rise in ID theft, privacy has once again returned as a barrier to adoption. With trust a vital component of a company’s brand, identity theft is a top priority for corporate officers and executives.

## **When Consumers Lose, Businesses Lose Too**

As we have shown, personal ID theft affects not only the individual, but also business revenue in unexpected ways. A study by ITRC showed the indirect financial impact on businesses. For example, the amount some victims have spent on recovery ended up having a profound affect on tourism and the hospitality industry. Credit limitations resulting from ID theft reduced victims’ vacation time by nearly two weeks per instance. The industry suffered a \$4 billion loss because consumers booked upwards of five million fewer vacations.

The business community as a whole loses when consumers experience ID theft. One estimate is calculated by multiplying the total number of victims (7 million) by the average loss \$17,000 (from the Florida Grand Jury Study), resulting in \$119 billion per year in fraud costs to businesses. The FTC estimated business losses at \$48 billion, but that is low because many people did not report the loss to them. The ITRC finds both these figures to be low. Based on reports they received from consumers, the average loss is more in the range of \$39,863, totaling \$279 billion, and this figure does not include any expenditure by businesses for attempted recovery.

Companies, schools and state governments are equally at risk. In one incident, the State of California recently learned that its entire employee database, with some 260,000 workers, was exposed to a hacker.

## **Why More Companies Aren’t Taking Action**

Electronic Data Systems Corp. and the International Association of Privacy Professionals recently commissioned the Ponemon Institute to conduct a study on privacy and identity management to gain insight into consumer preferences with regard to issues such as data security, awareness of technology, information hygiene and trust. The results, showing that consumers value convenience over privacy and security, have created some controversy among privacy advocates.

The survey of 1,041 U.S. consumers finds that 61 percent don't want to be forced to change their passwords on a recurring basis. Also, 57 percent did not want their accounts locked down after three failed attempts to validate identity. However, 85 percent agree that they should be denied access if a company can't validate their identity.

James Walsh, co-author of the book *Identity Theft: How to Protect Your Name, Your Credit and Your Vital Information...and What to Do When Someone Hijacks Any of These*, says naiveté is leading to a lax consumer attitude toward security.

“The expectation of security breeds complacency,” Walsh states. “The key is changing consumer expectations. Consumers want ease of transaction over greater security because they foolishly think [ID theft] can't happen to them.”

Walsh also states companies need to work toward educating consumers about how easy it is access information, but they still need to bear the responsibility of providing better care of customer information. He uses recent database thefts at AOL and Acxiom as examples of how easy it can be for thieves to steal valuable data. When more consumers understand the risks of ID theft, their attitudes will change. An unfortunate result of consumer disinterest is that companies will delay taking action to protect their stored data.

One of the biggest challenges privacy professionals face is getting a seat at the boardroom table. According to International Association of Privacy Professionals (IAPP), privacy experts from a variety of industries have shared how difficult it has been to get privacy on the minds of senior management to boost it as a corporate strategy.

## **Data Security: What Is Your Company Doing About It?**

In the following sections, we present in detail some ways information theft has affected companies and their consumers. While the issue of regulation has come to the forefront, fewer than five percent of Fortune 1000 companies are treating privacy as a strategic business issue. The reason for this may be the poor correlation between customer identify theft and corporate financial risk, which is due in part because executives are just beginning to understand the connection between a customer's personal losses and business losses. If consumers lose confidence, or worse yet, have their credit destroyed, they will in effect stop buying. Companies in a tight, competitive marketplace, working towards customers-for-a-lifetime, cannot afford to compromise customer confidence. Thus, the burden to protect consumers from identity theft must shift from the shoulders of consumers to those of the business community.

In the coming decades, it is vital that members of the business community examine their policies on information handling and adopt and implement better information handling processes. As it stands now, government agencies pass laws that seek to force companies to shred documents prior to tossing them in the trash. However, identity theft in today's world is largely handled electronically. Dumpster diving is old school. New laws need to address the current reality that electronic data theft is the most critical aspect of the problem.

## **The ChoicePoint Crisis: The Tip of the Data Disaster Iceberg**

According to Jonathan Penn, Forrester Research analyst, ChoicePoint didn't invest enough. "Choicepoint investment should have included educating and training employees to understand the value of the information ChoicePoint trades rather than simply look at its consumer profiles as a commodity. Companies have to look beyond the technology; technology only does what you tell it to do."

The ChoicePoint story is a good example of what can happen if a company does not heed data privacy and identity theft issues. Not only do companies collect data from their own customers, but they also buy data from commercial data brokers. ChoicePoint is the largest of these brokers, but there are hundreds that collect and sell private information for profit. Until recently not much attention had been placed on the issue of customer data security. In the past, the FTC received some reports on identify theft, but not enough to notice the epidemic it has become.

Just when consumers were beginning to gain more trust with online spending, the worst of all nightmares occurred. Thieves, posing as small business customers, gained access to ChoicePoint's database, compromising the personal information of 145,000 Americans. (ChoicePoint has about 19 billion records in total.) With the media attention given to ChoicePoint's lack of customer data protection, Pandora's Box opened, leaving companies and individuals at a huge risk.

With the recent rash of other high-profile disclosures of customer information loss at Bank of America and LexisNexis, the spotlight is now highlighting the risks companies face if they fail to secure their data. These risks include significant legal, financial, and public relations problems. Often all three will result from a significant breach of customer privacy. For instance, when ChoicePoint announced the fraudulent disclosure of 145,000 consumer records, its stock dropped nearly 20 percent and several shareholders filed lawsuits. On the other hand, a company can build a solid foundation of trust with customers creating a competitive advantage, by recognizing and addressing privacy,.

*“Seven million consumers had new financial accounts created in their name. Eleven million consumers faced credit card fraud.”*

—Gartner, 2004

*“Even when you give your information to legitimate merchants, it’s only as safe as that institution’s safeguards.”*

—Betsy Broder  
FTC Identity Theft Expert

*“The Anti-Phishing Working Group has reported that phishing attacks doubled in the month of October and many of the sites are hosted from hijacked home computers. The Group reported 6,597 new phishing schemes, making the monthly growth rate 36 percent. Of the new e-mail messages 46 unique brands were targeted. 1,142 phishing sites were discovered more than double what was found in September.”*

—Source: BBC News

## FTC Study Reveals the Magnitude of Personal Identity Theft Crisis

When business leaders begin to understand the impact data theft has on their customers, they will want to rethink their data protection plan. No customers, no business. New studies by the FTC show nearly 10 million consumers were victimized by some form of identity theft in 2004. That equates to 19,178 per day, 799 per hour and 13.3 per minute. Consumers have reportedly lost more than \$5 million and businesses, seen as the secondary victim of identity theft, have lost more than \$50 billion.

The FTC concluded from a follow-up nationwide survey that throughout the past five years more than 27 million consumers have experience ID theft. Between 2001 and 2002, ID theft hovered between 11 to 20 percent.

According to a new study by Harris Interactive it increased to 80 percent between 2002 and 2003 and 95 percent of respondents do not see an end to this issue.

An example of how extensive this epidemic has become, illegal immigrants, using stolen social security numbers, have obtained \$420 billion in Social Security wages. The effects to government and private entities are staggering.

Imagine how your customers, who have taken extra precautions to guard their personal information, their names, social security numbers, tax ID numbers, credit histories and employment records, would feel if they found out their PII was being piled into wheelbarrows and sold to the highest bidder. These kinds of crimes have a severe consequence to not only the consumer, but to businesses and our economy despite whether criminals are stealing from companies, the government or the individual.

Identity theft is a crime that feeds on the consumer’s inability control who has access to sensitive information and how and whether it is safeguarded. The other pressing issue is that data records often contain misinformation that can result in the loss of a potential job, purchase of a home or automobile or worse yet, a criminal conviction. The FTC now reports that 85 percent of people do not know they are victimized by ID theft until they are denied credit or employment, are notified by police or collection agencies, or receive credit card bills they never ordered. To make matters worse, the average arrest rate in identity theft crimes is approximately five percent of all reported cases.

While Congress is poised to consider several pieces of identity-theft legislation, including laws designed to extend expiring provisions of the Fair Credit Reporting Act, the House of Representatives is promoting state-by-state legislation. And the credit industry is pushing to maintain the current federal standards because of the complexities that would arise from dozens of differing state protection laws.

While the government is beginning to recognize protection issues with commercial data brokers, companies need to take charge of the issue themselves. Companies have an interest, and duty, to protect and control the

use of collected customer information. Companies that are proactive in addressing privacy issues may emerge with a competitive advantage by securing their customers PII and thus their confidence, loyalty and their money.

## Zero Liability Does NOT Mean Zero Damage

California Public Interest Research Group (CalPIRG) and Privacy Rights Clearinghouse (PRC) recently published a landmark report, *Nowhere to Turn: Victims Speak out on Identity Theft* (see some below.)

While major credit card providers heavily promote “zero liability” for consumers who shop online (i.e., consumers are not liable for fraudulent charges), consumers themselves are responsible for correcting identity theft issues when their credit card is stolen. This can take years of paperwork, lost time, result in embarrassment and limited access to loans and ability to buy property or an automobile while they spend years cleaning up their misfortune. The study concluded that although the financial loss is significant, most consumers felt the greater impact was emotional. Stress, emotional trauma, lost time and damaged credit reputation, consumer agreed, were among the most difficult to deal with.

Victims reported feeling violated, helpless and angry. Here are other findings from the reports.

*“I was not able to rent a place and do not know if I will be able to get housing when the current lease my family members signed for me expires. I cannot get a mortgage or better my financial situation. As a result, my life is paralyzed.”*

—ID Theft Victim

*“My credit card company told me I was now a credit risk since my information was out there and they cancelled my perfectly paid platinum card without any notice. I was trying to use it at a store and the clerk told me it was cancelled. When I called the credit card company, even though their TV commercials said otherwise, they were nasty to me, blaming me for the ID Theft. Zero Liability, I don't think so...”*

—ID Theft Victim

- Average total fraudulent charges added up to \$18,000, with ranges from \$250 to \$200,000
- Victims spent endless hours-- 1,000 to 11,520 hrs -- (42 to 480 days) trying to resolve the problems caused by the identity theft
- Victims spent between \$800 and \$40,000 hiring companies to help resolve the ID theft issue
- Only 45 percent of the victims had solved their ID theft case and it took two years
- 55 percent of the victims cases remained unsolved and had been open for four years
- 76 percent were victims of “true name fraud”, where thieves had opened an average of six new fraudulent accounts in their names
- 67 percent felt the credit bureaus were ineffective in removing fraudulent accounts on their records or in placing a fraud alert on their report
- 46 percent had fraud occur after placing a fraud alert on their credit report
- 12 percent were subjected themselves to criminal investigations of which they were not guilty of
- 49 percent missed work as a result of trying to resolve the ID theft issue (from 1 to 12,800 hours of lost labor hours per person)
- 37 percent used vacation or personal leave time (up to 1,000 hours)
- 21 percent reported lost work time due to seeking related medical services (2 to 10,000 hours per person)

Fact: bad word of mouth is one of the most influential methods of communications among consumers. With that in mind, the burning questions executives need to be asking themselves are: If consumers are this leery about ID theft, how many will be willing to increasingly shop on the web, disclose personal information and place orders over the phone? Could ID theft dry up multi-channel sales call centers in an instant?

## Conclusion

Studies show ID theft is on the rise and more costly than ever. Consumers are increasingly becoming weary of online financial transactions and companies and the government is lagging to correct current trends. All parties, consumers, businesses, and the government need to pay more attention. If companies don't protect their customer's data, they might not be able to maintain the trust required to be able to continue to collect and use the data. With the trend being

increasingly more data theft, customers may opt to stop shopping online or over the phone. Because these are two huge revenue sources for most businesses, a strategic position on data collection and protection is now a business necessity.

If data protection is something that your company is focusing on, you may want to read our second whitepaper on customer data protection. In part II, we address strategies on how a company can get a handle on their current data privacy and protection status. Also, we will look at how to begin creating a more secure environment so that you can maintain your current customers (which are less expensive to maintain than to acquire new ones) and remain in this position in the highly competitive market place.

## About The Authors



**Brian R. Johnson**

*Managing Vice President, Customer & Channel Solutions*

As a managing vice president for Hitachi Consulting, Mr. Johnson is responsible for profitable growth and intellectual property development in the areas of sales and channel, marketing, and customer care optimization and automation. Mr. Johnson has spent his entire 20 year professional career assisting companies with improving and automating their customer facing functions.

Mr. Johnson has extensive experience in helping clients develop CRM strategies, architect technical CRM solutions, plan for complex global implementations, and manage the process and organizational change required to successfully transform themselves into customer-centric organizations.

Prior to joining Hitachi Consulting, Mr. Johnson spent ten years leading commercial software development teams in the creation of software for sales, customer service, direct marketing, field service, human resources, and financial applications.

Mr. Johnson holds a Bachelor degree in Computer Science and Economics as well as an MBA in Information Systems from the University of Colorado. Mr. Johnson is a Ph.D. Candidate in Applied Management and Decision Sciences at Walden University.



**Natalie L. Petouhoff**

*Senior Manager, Customer and Channel Solutions*

Dr. Nat, a senior manager for Hitachi Consulting, is responsible for writing cutting-edge books, articles and white papers that provide companies with mission-critical information to transform their business strategy. Dr. Nat's years as an innovator and thought leader have provided companies with the unconventional practical discipline necessary to guide companies to rethink their customer strategies. That rethinking includes shifting paradigms from the *value*

*the customer brings to them to the value a company can bring to a customer,* which affects the Customer Experience, Customer Advocacy and Customer Lifetime Value. Known on the speaking circuit as Dr. Nat, she is invited for book signings and keynotes at industry conferences like the Gartner CRM Summit.

Dr. Nat has 15 years of experience in technology implementations, focusing on CRM, Contact centers, ERP and Share Services Systems, sales and marketing. Dr. Nat helps clients create their own, unique customer experience, increasing their Customer Lifetime Value. As a Business Process Reengineering and Change Management expert, she is able to help manage projects so that they provide a high rate of return, stay within scope, on budget and on time. As a professor in Pepperdine's Business School, she taught Change Management, Leadership, Project Management and Organizational Behavior and Design.

Dr. Nat obtained a Bachelor and Masters Degree in Metallurgy and Material from the University of Michigan. She was awarded the General Motors Fellowship to complete her Doctorate of Engineering from UCLA where she did her thesis research at Oak Ridge National Laboratory and Hughes Research Laboratories in Metallurgy and High Energy Particle Physics.

## References

- Turner, E. C., & Dasgupta, S. (2003). PRIVACY ON THE WEB: AN EXAMINATION OF USER CONCERNS, TECHNOLOGY, AND IMPLICATIONS FOR BUSINESS ORGANIZATIONS AND INDIVIDUALS. *Information Systems Management*, 20(1), pp8-19.
- Cranor, L., & Reagle, J. (1997, December 27-29, 1997). *Designing a Social Protocol: Lessons Learned from the Platform for Privacy Preference Project*. Paper presented at the Telecommunications Policy Research Conference, Alexandria, VA.
- Cranor, L. F. (2002). *Web Privacy with P3P*. Sebastopol, CA: O'Reilly & Associates, Inc.
- Cranor, L. F. (2003, March 2003). *The Role of Privacy Enhancing Technologies*. Retrieved April, 2005, from <http://www.cdt.org/privacy/ccp/roleoftechnology1.shtml>
- Harris Interactive. (2001, December 2001). *Privacy Notices Research Final Results*, from <http://www.ftc.gov/bcp/workshops/glb/supporting/harris%20results.pdf>
- Olmstead v. United States (U.S. Supreme Court 1928).
- Turner, E. C., & Dasgupta, S. (2003). PRIVACY ON THE WEB: AN EXAMINATION OF USER CONCERNS, TECHNOLOGY, AND IMPLICATIONS FOR BUSINESS ORGANIZATIONS AND INDIVIDUALS. *Information Systems Management*, 20(1), pp8-19.

## About Hitachi Consulting

As Hitachi, Ltd.'s (NYSE: HIT) global consulting company, Hitachi Consulting is a recognized leader in delivering proven business and IT solutions to Global 2000 companies across many industries. We leverage decades of business process, vertical industry, and leading-edge technology experience to understand each company's unique business needs. From business strategy development through application deployment, our consultants are committed to helping clients quickly realize measurable business value and achieve sustainable ROI.

Hitachi Consulting's client base includes nearly 30 percent of the Fortune 100 as well as many leading mid-market companies. We offer a client-focused, collaborative approach and transfer knowledge throughout each engagement. For more information, call 877-664-0010 or visit [www.hitachiconsulting.com](http://www.hitachiconsulting.com).

Hitachi Consulting – Inspiring your next success!®

## About Hitachi

Hitachi, Ltd. (NYSE: HIT), headquartered in Tokyo, Japan, is a leading global electronics company, with approximately 326,000 employees worldwide. Fiscal 2003 (ended March 31, 2004) consolidated sales totaled 8,632.4 billion yen (\$81.4 billion). The company offers a wide range of systems, products and services in market sectors including information systems, electronic devices, power and industrial systems, consumer products, materials and financial services. For more information on Hitachi, please visit the company's Web site at <http://www.hitachi.com>.

###

© 2006 Hitachi Consulting Corporation. All rights reserved. "Inspiring your next success", "Knowledge-Driven Consulting" and "Information Velocity" are registered service marks of Hitachi Consulting Corporation. Printed in USA.