1 Motivate the Troops

People don't change bad habits until they have a compelling reason. Too often that compelling reason is the result of a habit's negative outcome; but the promise of positive rewards resulting from the establishment of good habits can be a strong motivator. In the workplace, aligning responsible information stewardship with personal *and* professional gain can set the stage for good privacy habits.

Let My Failure Motivate Your Change

At breakfast on the morning of August 12, 2003, a small and profitable computer company thrived at the foot of the Rocky Mountains. By lunchtime that day, that same business was on its way to ruin. Within 12 months, due to the theft of personal and company information, a 40-year-old family-business-turned-software-startup was doomed, and John, heir to the prosperous enterprise, faced the prospect of prison for crimes he didn't commit.

Beyond the specter of prison time for John, the situation held dire consequences for his family and friends. There was a real threat that his wife and two young daughters might be separated from their husband and father, if John went to prison. John's parents, who founded the company in 1964, shouldered most of the financial responsibility for the dying business and experienced declining health from the resulting stress. In the end, the situation would expose a dark secret kept by John's close friend, Doug, a recent partner in the business.

It sounds like fiction, and sometimes when I'm recounting the ordeal in front of an audience, it *feels* like fiction. But it's 100 percent true. This is the story of how a failure to understand the importance of data privacy not only destroyed a healthy business, but nearly took down an entire family, as well.

If you haven't already figured it out, I am John Sileo, the business leader whose naïve choices brought about the sad saga. Before I experienced it firsthand, I didn't understand that both *individual and business data privacy* are integral to running a profitable company.

What happened to my business, and to me, is more common than you may realize. The statistics throughout this book prove it. The stories I hear from my audiences prove it. But the media headlines continue to ignore it. They minimize massive breaches such as those that occurred at TJX, Heartland Payment Systems, and the U.S. Department of Veterans Affairs with sterile, unemotional language, and they talk about the *risk* of identity theft, but rarely do these stories assess the true toll of identity theft and put a human face on this crime.

Why is the human element missing from these stories? One reason is that victims are often ashamed to openly share their mistakes and failures with the world. Identity theft and its consequences can be humiliating, causing victims to remain quiet. Another reason is that corporations don't want the true emotional costs of information crimes exposed, for fear doing so will awaken a sleeping giant—the complacent public—and you and I might not stand for it any longer. So they call the crime a "data breach," to make it sound technical, hence impersonal. We stay silent, and the business world makes it about numbers instead of lives. But identity theft, or whatever you choose to call it, is highly personal, incredibly invasive, and deeply violating.

There is a great irony underlying the division of this problem between individuals like you and me, and businesses that experience data breach, such as Heartland. We are one and the same. The CEO, responsible for the corporation's data at the highest level, has a Social Security number that is vulnerable to theft. The executive in charge of computer systems that might be hacked, and laptops that might be lost, has a family whose personal medical records could be on those systems. Every human resources administrator responsible for employee records is also an employee whose private financial information is stored in similar files. Every janitor who disposes of sensitive identity documents in the dumpster has identity documents of his own that could be improperly discarded in the trash.

Therein lies the first step in our solution: You must recognize that you could be the victim of this crime just as easily as you could be the source. You are the CEO, the IT manager, the HR administrator, the janitor, the employee, *and* the individual.

Corporate data privacy starts by training a roomful of potential identity theft victims. Teach the CEO and the janitor to understand the destructive emotional and financial impact in personal, human terms that relate directly to them (e.g., the loss of their *own* medical records) and you have the foundation for an effective privacy leader at any level of the organization.

I was forced to make this connection between personal responsibility and workplace responsibility by being the victim *and* the source. I share my story here both as John Sileo, husband and father, and as John Sileo, business executive, so that my pain can guide your progress. Your responsibility is to let my failures motivate and inform your change. I am the example you can hold up to your employees and yourself so that all of you come to understand the consequences of the apathy, ignorance, and inaction that make this a difficult crime to avoid.

This is why you need to read this book, whether you are an individual concerned about guarding your financial well-being or a business leader who is responsible for maintaining the trust and reputation that your employees and customers have placed in you. *You could just as easily be the source as the victim, and it is your responsibility to protect against both.*

The Three Enemies of Privacy: Apathy, Ignorance, and Inaction

When it comes to identity theft and data breach, I'm guessing that your first response is to do nothing. After all, you think, *it's not your fault; it's not your responsibility; it's too difficult a problem*. You have been trained in the behavior of **apathy**: to care little about protecting your private information. In fact, you have been conditioned to give it away without a second thought, armed with excuses as to why you don't need to act: "It won't happen to me." "I'll get to it later." "It's out of my control."

Rubbish.

It is human nature to invest time to prevent tragedy only *after* we've experienced the pain that results from apathy. We hop on the treadmill and order from the healthy menu only *after* our heart screams for attention. We install a

home security system only *after* we've been robbed. Pain motivates action, but the damage is usually done.

> *If you know what matters to you, it's easier to commit to change. If you can't identify what matters to you, you won't know when it's being threatened. And in my experience, people only change their ways when what they truly value is threatened.*
>
> *—Marshall Goldsmith, What Got You Here Won't Get You There (pp. 29–32)*

Similarly, we come to grasp the true value of our personal information only *after* an identity theft or data breach incident occurs that affects us. When your bank calls to tell you that your ATM number was skimmed and your account emptied by a criminal in another state, or when the IRS informs you that your recent tax filing was incorrect because an undocumented worker obtained employment using your Social Security number, the problem becomes personal and you've got a mess on your hands. The good news is that your willingness to read *Privacy Means Profit* sets you apart from the apathetic crowd. By buying this book and learning more about the problem of identity theft, you have taken the first step toward protecting yourself, personally and professionally.

I wasn't so lucky: I ignored my first minor identity theft "heart attack." Just months before my business was destroyed by data theft, I disregarded a warning that should have awakened me to this crime. Days after moving into a new neighborhood, a woman stole my identity out of a garbage bag full of unshredded home-loan documents. "They're just harmless copies," I thought to myself as I threw them out. I didn't even consider identity theft, and I certainly didn't own a shredder.

Using my Social Security number to gain access to my credit profile, the thief purchased her first home (my second) in another state. Unable to keep up with the mortgage payments, she defaulted on the loan and started bankruptcy proceedings—in *my* name. The police declined to investigate (too much of a backlog, they claimed) and I was left alone to endure hundreds of hours cleaning up the mess, filing police reports, repairing my credit, dealing with collection agencies—all on my dime. I ended up spending many weeks of hard-earned vacation time recovering from a crime that could have been prevented with only minutes of effort. My **ignorance** about the real costs of

this crime, and even the most basic means of prevention, meant that I had to learn firsthand, the hard and expensive way.

You can learn from my failures, and from the knowledge I gained in the process. In my experience, the most successful people (as measured by happiness, income, and peace of mind), and the most successful businesses (as measured by profitability, customer loyalty, and employee satisfaction) understand that it is easier and *far less expensive* to prevent a disaster than to recover from one. It's why we exercise, teach our kids to respect fire and avoid strangers, diversify our financial investments, and stay out of dark alleys in rough neighborhoods. It's why businesses back up data, perform criminal background checks on job candidates, and provide employee training about many types of risk prevention.

It's no surprise then that successful corporations and insightful individuals apply this same prevention-minded strategy to secure one of their most valuable assets: information. They realize that, in a world where information is currency and knowledge is power, *privacy means profit*.

Privacy means profit applies to both individuals and businesses. The more effectively you protect your private information, the more secure your finances—your personal net worth or your organization's bottom line—will be. I lost nearly $300,000 to identity theft and data breach, and that doesn't even account for the two years I spent recovering rather than earning a salary. Consider the following statistics that illustrate why *privacy means profit*:

- The TJX data breach loss was estimated at *$4.5–$8.6 billion*,[1] at $100 to $182 per breached record, as estimated by experts.
- Heartland Payment Systems stock value declined *64 percent* in the days after it acknowledged a data breach.[2]
- The average data breach costs *$6.75 million* (see Figure 1.1).[3]
- The number of breaches are up *47 percent in a one-year period.*[4]
- In 2008, *285 million records* were breached.[5]
- Of individuals affected by a data breach, *31 percent* will terminate their relationship with the company that lost their information.[6]

The math behind the profitability of privacy is as simple as a profit-and-loss calculation:

$$\text{Revenues} - \text{Expenses} = \text{Profit}$$

Data Theft = Significant Expense (stock depreciation, customer attrition, lawsuits, victim credit repair, brand damage)
Theft Recovery Expenses > Prevention Expenses

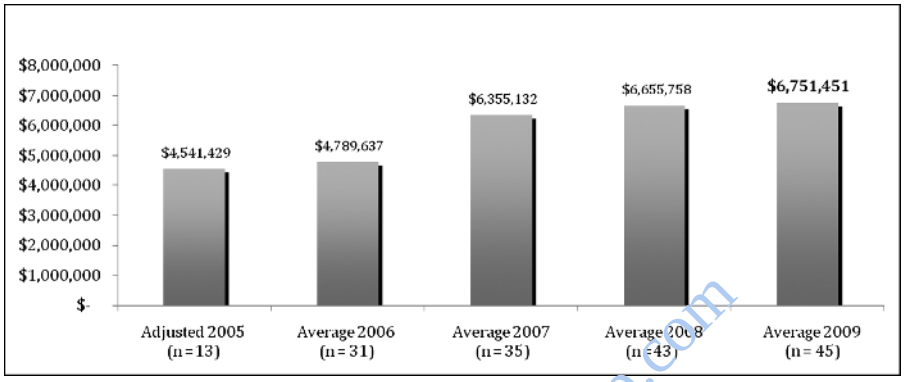

FIGURE 1.1 Average Total Cost of Data Breach by Year

Source: "Fifth Annual U.S. Cost of Data Breach Study," 2010, Ponemon Institute.

In other words, *safe data is profitable data*. And protecting customer data, employee records, and intellectual property isn't just good business, it's the right thing to do.

Despite experiencing the actual costs of identity theft at a personal level at the hands of a dumpster diver, initially I did nothing to further protect myself, nor did I adapt and apply my knowledge at a business level. I gave in to the final enemy of privacy: **inaction**. It was my refusal to adapt what I had learned personally to a broader sphere of privacy as it applies to business that brings us back to the sunny morning of August 12, 2003.

Inaction Destroyed My Business

It was my business decision to form a joint venture with Doug, a business colleague who had become a close friend while consulting to my computer company. Together, we built an Internet software business that was profitable by its third month, providing the lion's share of revenue sustaining our operations and 11 employees. I was entranced by how profitable we were, by the financial upside of being a successful entrepreneur in a hot industry, and by how easily it all came together.

It seemed too good to be true. And so it was.

In the headiness of our success, I failed to verify the credentials of my new friend and business partner. I didn't thoroughly interview his references, question his willingness to jump ship from a stable and lucrative job to a highly risky venture, or perform even a simple criminal background check. It didn't seem necessary; after all, Doug worked harder and for longer hours than anyone else in the company. Eventually, I gave him access to the company computer systems, accounting software, and bank accounts. He knew many of my passwords, had access to personal files in my office, and enjoyed the privileges of trust with little monitoring of his activities. He was such a good fit as a business partner that my wife and father both commented prophetically that he was *too good to be true*. At one point, my father even advised that he wouldn't put his trust in a business partner until that trust was earned, and that earning trust should take at least five years.

I agreed, but thinking something and acting on it are two entirely different things.

I realize that handing over so much control so quickly must seem terribly naïve to you—and it was (in this case, naïveté that was the by-product of *apathy*, *ignorance*, and *inaction*). Yet I see the same story replay itself over and over again in businesses much larger than mine. After all, Doug was a friend and a very intelligent man, and he knew how to use those qualities to *engineer my trust*. We worked together almost two years before he started taking advantage of me, all the while treating me like family.

Doug used my unprotected identity and the company's private customer data to embezzle nearly $300,000 from our clients over the course of 18 months. On August 12, 2003, during a phone call, our biggest client threatened to put me in jail for the thefts, since it was my name that appeared throughout the criminal paper trail. Several days later, an investigator from the Denver District Attorney's office contacted me and started what would become a two-year battle to prove my innocence and stay out of jail.

During that time, our software business failed (despite being profitable even without embezzled income), the 40-year-old family computer business failed, and I lived under the constant cloud of possibly going to prison for crimes I didn't commit.

I was, however, guilty of one thing: refusing to take responsibility for the safety of personal and business data.

Despite the huge financial losses we suffered, the most painful aspects of this ordeal turned out to be the two years of quality time I lost with my wife and kids while fighting business battles, the negative effects it had on my parent's health, and the deep bitterness I felt at being betrayed by a close friend. *Money can always be earned back; time and relationships cannot.*

After a stint in a psychiatric hospital, Doug eventually went to jail, but for only 18 days. His sentence didn't feel like justice to me; nevertheless, and even after all he put me and my family through, I made the decision to focus on *what I could control* rather than the severity of Doug's punishment. After two cases of identity theft and two years of recovery, I finally took responsibility for protecting my identity and the identities touched by my business.

Eventually, from the ashes of my former profession rose a new career, a new life, and a new respect for privacy. Passing what I have learned on to audiences around the world—and to you—is the only fitting justice for this ordeal.

Business Relevance

As a business leader, it is essential that you clearly understand the relationship between identity theft, data breach, and your bottom line. Here is a crash course, from my perspective.

One of the costliest data security mistakes I see executives make is to initially approach data privacy from the perspective of the company. They don't recognize the following reality: *All privacy is personal*.

In other words, no one in your organization will care about data security, privacy policies, intellectual property protection, or data breach until they understand *what it has to do with them*. If your employees and executives don't care about protecting their own identities (to prevent identity theft), how can you expect them to care about protecting corporate identity (to prevent data breach)? Like the emergency oxygen masks on a depressurized airplane, it's important to put your own on first, or you'll be worthless to those around you. *Protecting yourself first isn't self-centered; it's effective and educational*. Security begins at the human level and expands outward to the group level.

I recently delivered a speech at the Pentagon as part of an ongoing financial literacy campaign run by the Department of Defense. After the speech, an Air Force commander asked me why he was having such a hard time convincing his younger soldiers to protect sensitive military data. Their risky behavior included inadvertently tweeting troop locations, posting photos of fellow soldiers on their Facebook walls, and surfing on unprotected wireless networks. The problem, which has been publicly documented, has led the Pentagon to ban social networking from at least one branch of the military (at time of publication).

When I asked the commander how many of his men and women had been trained to understand the value of protecting their own personal information (i.e., how many had just attended the financial literacy event), he immediately drew the connection: *Good personal privacy habits lead to good professional privacy practices.* Change always takes place at the personal level first.

The end game for business leaders is to build a Culture of Privacy within their organizations, to make security part of the daily fabric, part of the mission and vision of their companies. A Culture of Privacy exists when every member of the organization (especially the CEO) *believes* in the need to protect his or her own private information, *as well as* customer data, employee records, and intellectual property.

This foundation of belief is clearly lacking among corporate executives. Look at the key findings of the Ponemon Institute/Ounce Labs study, "Business Case for Data Protection," which surveyed C-level executives (CEO, CFO, COO, CIO, CSO, etc.) about data protection inside of their corporations (emphasis mine):

- Of the C-level executives surveyed *82 percent* said that their organizations had experienced a *data breach*, and many of them are *positive they cannot prevent a repeat performance*.
- Of the CEOs surveyed, *53 percent* said that the CIO is responsible for data protection, yet only *24 percent* of the other C-levels would point to the CIO as the one responsible for data protection overall.
- Of those who are said to be in charge of data protection, *85 percent* don't believe that a *failure to stop a data breach would impact their job*.

(*continued*)

(*continued*)

In other words, C-level executives admit that a breach has already happened, are fairly certain it will happen again, recognize they are unprepared to stop a recurrence, and yet can't clearly identify who will be held responsible; nor do they feel that they will be held accountable when the inevitable happens. At this stage, building a Culture of Privacy is mostly bluster.

The result is that many organizations try to implement privacy policies and practices without actually believing in their mission. Instead of fostering a voluntary Culture of Privacy, they end up force-feeding an involuntary Regime of Privacy, and fall back into apathy when the fear wears off.

The most effective way to build a Culture of Privacy is to break it down into three simple steps (most corporations skip the first step, dooming them to failure):

1. *Motivate the individual.* Train your employees and executives on how to protect their own information *first*. Learning the basic principles of privacy at an individual level is a prerequisite for all subsequent forms of data security, and supplies the necessary motivation to apply the same habits at work. All employees need to overcome their own apathy, ignorance, and inaction before they are equipped to protect corporate assets. *This book is aimed at making it personal. By learning to protect their own identities, your executives and employees are acquiring the building blocks necessary to construct a corporate Culture of Privacy*. Identity theft training is good for their wellness, and is a means to a safer and more profitable end.
2. *Empower the team.* Employees alone do not have the authority or resources to act. By empowering cross-departmental teams (who already understand privacy at a personal level) with the authority and resources to focus on low-hanging security fruit (e.g., laptop computers, document shredding, wireless surfing), you make immediate progress and win crucial organizational buy-in. In contrast, organizations with a Regime of Privacy tend to force data security into a silo (e.g., "It's the IT department's responsibility"—see

statistics cited previously), never taking into account the vital role played by legal counsel, compliance officers, the CFO, human resources, and even facilities maintenance. In a Culture of Privacy, the team is integrated, and the results are more enduring.

3. *Lead by example.* There is nothing that undermines a Culture of Privacy faster than an executive team that doesn't practice what they preach. A CEO who surfs unprotected in the airport, or refuses to invest in deskside shredders, will send a hypocritical message echoing throughout the corporation: "Privacy doesn't really matter; we're just going through the motions." In the same manner, a CEO who appoints some form of chief data protection officer but doesn't supply the vision, budget, or authority to make it happen is the same CEO whose data breach catastrophe shows up on the front page of the *Wall Street Journal*.

Look closely at the Contents for *Privacy Means Profit*. The chapter headings provide a road map for the individual steps to take in building your Culture of Privacy. Begin with a privacy boot camp, where you *motivate* change before you demand it. *Define* what data is at risk, where it lives, and why it needs to be protected. *Engage* your troops with simple, memorable tools. During basic training, teach them to *eliminate*, *destroy*, *secure*, *lock*, *evaluate*, *interrogate*, and *monitor* at-risk information. Don't try to implement the strategy overnight. Instead, target the enemy by *adapting, accumulating, and prioritizing* your security campaigns. These are the skills you will develop at a personal level by reading the remainder of this book.

How to Get the Most Out of This Book

You will notice that this book is organized differently from other books on identity theft, which are typically structured around tasks and to-do lists (e.g., protecting your mail, shredding documents, etc.). While *Privacy Means Profit* covers all of those tasks in the Action Items feature of each chapter, it embeds them within broader concepts of protection such as *eliminate*, *destroy*,

lock, and so forth. These mind-sets can then be easily adapted and applied in the workplace.

By training you at the conceptual level and reinforcing what you learn with very specific action items to complete, you will walk away with a much broader and more flexible understanding of protecting yourself and your workplace. Giving you only checklists won't protect you over the long term, because identity thieves change their methods of attack, rendering any static checklist obsolete as soon as it is printed. By learning the concepts, you will have a dynamic skill-set to apply both today and in the future, at home and at work.

Each chapter contains three features:

The Mind-set: The first layer of protection is a mind-set, or a habitual way of thinking about your private information that will trigger alarms in your head when your identity is at risk. For example, instead of having to remember to shred lists of specific documents, you will develop the habit of destroying any private information that will be handled by others. I describe this mind-set as "think like a spy," and I will explain it in detail in Part II.

Action Item Checklist: The second layer of protection is a series of specific action items (to-do steps) that should be completed to protect your personal identity. I use the action items in each chapter to illustrate and reinforce exactly how you start to think like a spy. When you are shredding old bank statements, for example, you aren't just checking an item off your action list. You are reinforcing the habit of destroying anything with a piece of your identity on it that you no longer need. These action items are based on statistical data showing how identities are most commonly stolen and who steals them. The action items provide the most immediate and practical form of protection.

Business Relevance: In relevant chapters, I bridge the knowledge of how to protect yourself personally with how to expand that into your workplace. For example, once you have learned to properly shred sensitive documents at home, it is much easier to apply a more sophisticated form of shredding at work. This feature is targeted primarily at business leaders who are trying to protect their organizations against data breach and workplace identity theft, but it will be informative for individuals as well. *If you are an employee at a corporation, association, university, or*

small business, you must realize that protecting organizational data is vital not only to your company's profitability, but for your job security.

Give a man a fish and you feed him for a day. Teach a man to fish and you feed him for a lifetime.

—Lao Tzu

By reading *Privacy Means Profit* both for the concepts as well as the action items, you will learn to "fish" for yourself. If you are anxious to complete the checklists first (i.e., feed yourself today), skip to Chapter 16, "Prioritize Your Attack: The Privacy Calendar," and return to the other chapters as you have time.