Harvard Business Review
www.hbrreprints.org

HBR Case Study and Commentary

How should the Flayton Electronics team respond to the crisis?

Four commentators offer expert advice.

Boss, I Think Someone Stole Our Customer Data

by Eric McNulty

Reprint R0709A

Flayton Electronics learns that the security of its customer data has been compromised—and faces tough decisions about what to do next.

HBR CASE STUDY

Boss, I Think Someone Stole Our Customer Data

by Eric McNulty

Brett Flayton, CEO of Flayton Electronics, stared intently at a troubling memo on his desk from the firm's head of security. Running his hands through his full head of barely graying hair, he looked not unlike his father did when he established the first Flayton Cameras and Stereos 25 years ago.

The security situation had come to Brett's attention just before nine o'clock the previous evening. On his way home from a vendor meeting, he had been settling into an armchair in the airline lounge. He had barely opened *Electronics News* when his mobile phone rang. It was Laurie Benson, vice president for loss prevention.

"Brett, we have a problem. There might be a data breach." Laurie, a tough but polished former Chicago police detective, had been responsible for security at Flayton's for almost three years. She had an impressive record of reducing store thefts while building productive relationships with local schools, community groups, and law enforcement.

"What kind of data breach?" Brett asked. His tone was calm, as always, yet he scanned the lounge to make sure that no one could overhear.

"I'm still not sure," Laurie admitted. "I was contacted by Union Century Bank. They regularly examine their fraudulent accounts for patterns, and we've shown up as a common point of purchase for an above-average number of bad cards. They're getting me more information, but I thought you'd want to know right away. It could be nothing—or it could be significant."

Brett recalled the newspaper stories he had read about stolen laptops with veterans' records stored on them and about hackers trying to penetrate eBay and other big online retailers. His firm was just a regional chain with 32 stores in six states and a modest online presence. Flay-

HBR's cases, which are fictional, present common managerial dilemmas and offer concrete solutions from experts.

ton's could hardly be a target for stealing lots of customer data. Or could it?

"Laurie, I'm not sure I understand. People were using stolen credit cards at our stores? Our clerks weren't checking cards correctly?"

"No," she replied earnestly. "It looks like we might be the leak."

New Territory

Back in his office the next morning, Brett surveyed the fruits of his own overnight Internet research. Data theft was apparently common, and companies could be breached in various ways. The thieves stole credit card information, social security numbers, bank account information, and even e-mail addresses. There seemed to be a black market for almost any kind of data. He learned that the criminals were becoming increasingly clever and that no one was immune. He took some comfort in his company's having recently spent considerable time and money becoming compliant with new payment card industry, or PCI, standards for data protection.

Laurie sat across from Brett in silence. She had anticipated this kind of theft would happen sometime, but actually coping with it was new territory for her. All of her related professional experience had involved the stealing of physical property. In this case, data had been obtained illegally by someone, somewhere—but with no clear-cut crime scene to sweep for clues.

A routine analysis by Union Century Bank of fraudulent credit card charges identified purchases at Flayton's on almost 15% of the cards in this particular batch of about 10,000 compromised accounts—so roughly 1,500 in all. It was a surprisingly high number for a routine check. Union Century had begun to notify other banks, as well as Visa and MasterCard, to see whether they had observed similar patterns.

"Wouldn't we have noticed that ourselves?" Brett asked. "We get regular reports from the banks."

"Not necessarily," Laurie replied. "We would have, if the purchases at Flayton's had been fraudulent. But that's not what seems to have happened. The purchases were legitimate, but the account information is being used elsewhere illegitimately. We could not have identified the problem, except through a random check like the one Union Century did. The 1,500 accounts could be just the tip of the iceberg."

"What's our potential exposure?" Brett inquired matter-of-factly. Quietly he wondered whether the firm's PCI compliance would provide sufficient protection.

"Not sure, I'm afraid. The credit card holders are protected by the bank, but what that means for us is tough to say."

"Why do we have to notify customers at all?" Brett asked, genuinely puzzled. "Haven't the banks already informed them that their accounts have been compromised?"

"It's not that simple," Laurie explained. "Some banks have sophisticated analysis tools to detect unusual patterns early on, but that method is imprecise. Often banks don't begin to recognize a problem until a bill goes unpaid or a credit card holder complains. They usually just monitor a situation until specific problems arise. If cardholders don't pay close attention to their bills, fraudulent debt could accumulate for months before it's caught. As I understand from the bank, alerting our customers that their data might have been stolen could be the best means of early detection."

Laurie had brought herself up to speed pretty quickly and had spent the early morning hours briefing key managers and flagging possible areas of vulnerability in the data chain. The chain itself was simple, but identifying its weakest points was not. At the cash register, a customer presented a payment card, which was swiped through a reader. The information from the card and the specifics of the purchase were transmitted to a bank for approval or rejection. It all happened in seconds. Transaction information was stored on company computers and showed up in a number of reports. Credit card numbers shouldn't have been stored in the firm's system, but Laurie still didn't grasp every step of the process. Could the card readers have been hacked? Could the data lines between the stores and the bank have been tapped? Were the stored data secure? Might someone have inserted code into the company's software to divert certain information to a remote computer—or even a computer on the premises? Could it have been an inside job? Or perhaps the work of someone who had been fired?

"Any chance that this could just be someone's careless mistake?" Brett volunteered. "Maybe an employee tossed files into the dumpster."

Eric McNulty (emcnulty@hbsp.harvard.edu) is the managing director of the conferences division of Harvard Business School Publishing, which publishes HBR, in Boston. His weekly online column, "Heard in the Suite," appears on Thursdays at www.harvardbusinessonline.org.

"Well," Laurie shrugged, "it's possible." She paused, then shook her head. "But not likely."

"What about some kind of coincidence?" Brett was grasping at straws. "Perhaps 1,500 of our customers just had the same bad luck?"

Laurie inhaled deeply, then exhaled slowly. "Anything's possible at this point. I need to know more than I do now. The bank connected me with the Secret Service, which is handling the investigation because accounts in multiple states were affected. It will take a couple of days to have other banks try to corroborate Union Century's findings. For now, the Secret Service recommends that we run background checks on everyone who could possibly have access to data on the scale of the breach—even people we've run checks on before. We should also pull personnel files on anybody we've let go in the past year for cause. And we need to check, check, and triple-check every system in the house."

"I'm sure that Sergei already has that in the works," Brett replied. He knew that kind of thing would drive Sergei Klein, the CIO, nuts until he figured it out. Brett rose and paced around the perimeter of his office. He paused at the window to survey the more than 300 cars in the parking lot. He felt some responsibility toward every person with a vehicle in that lot and toward the hundreds more who worked in the stores.

"What else did the Secret Service say to do?" Brett had visions of black SUVs with tinted windows, full of earnest agents in wraparound sunglasses, descending on his headquarters and stores.

"First," Laurie explained, "they asked that we keep this under wraps until we get a full picture. Now that the banks know what's going on, they can shut off the cards quickly when fraud surfaces. But the feds want enough normal activity to allow them to do a proper investigation and, we all hope, initiate prosecution. Although the Secret Service is taking the lead, they expect to also involve some state and local fraud units.

"But what about the customers? We can't knowingly let them be defrauded!" Brett was uncharacteristically adamant. "This business was built on trust. Our reputation for a square deal is a competitive advantage. I don't ever want to have to look a customer in the eye and defend not being straight with him."

"It's a question of the greater good," Laurie offered. "The customers will not be responsible for the charges. They're fully covered. We have to nail the bastards who did this."

"This business was built on trust. Our reputation for a square deal is a competitive advantage. I don't ever want to have to look a customer in the eye and defend not being straight with him."

Limited Defenses

Brett couldn't bear to just wait for answers. He quickly ushered Laurie out of his office, canceled his next meeting, and made his way past a dozen gray cubicles toward Sergei's haunt. Listening to the sounds of fingers clicking on keyboards and file drawers opening and closing, he couldn't help but marvel at how much information was available to anyone in those cubicles at any time.

As Brett arrived at Sergei's door, the CIO was slamming down his phone in frustration. Brett's attention shifted from the receiver directly to Sergei's eyes. Sergei swallowed.

"Sergei, what do we know?"

"We're still trying to determine what happened," the CIO offered meekly.

"But we are *sure* that our PCI systems were working, right?" Brett pushed.

"Becoming PCI compliant is complicated," Sergei hedged, "especially when you're constantly improving your own technology." He ran through a laundry list of the complexities of recent improvements. At any given moment, Sergei had three or four high-priority tech projects in various stages of implementation. It was a constant juggling act.

Brett, in a rare display of anger, pounded his fist on Sergei's desk. "Are you saying, Sergei, that we're not actually PCI compliant?"

Sergei stiffened. "We meet about 75% or so of the PCI requirements. That's better than average for retailers of our size." The response was defensive but honest.

"How have we been able to get away with that?" Brett growled. He knew that PCI compliance, which was mandated by all the major credit card companies, required regular scans by an outside auditor to ensure that a company's systems were working—with stiff penalties for failure.

"They don't scan us every day," Sergei demurred. "Compliance really is up to us, to me, in the end."

Core Values at Risk

The wall across from Brett's office was covered with hundreds of photographs taken with cameras bought at Flayton's. Weddings, vacations, graduations, sunsets, and smiling

infants—all sent in by customers. Similar displays brightened the walls of every Flayton Electronics store, to remind employees that customers are not just wallets who buy your products. One of the pictures closest to Brett's doorway was of his father handing over a poster-size check to a local charity.

As Brett contemplated the photos, he wondered whether he had pushed growth too quickly. After his dad retired, Brett ramped up his ambitions. He had sought private equity investment a few years ago, and he was constantly aware of his obligation to deliver the returns he'd promised. His strategy had been aggressive, but he was confident in it—until now. Had he been shortsighted about the infrastructure needed to run a much larger company? Had his company's needs outgrown the capabilities of his longtime staff? Had he left Flayton's vulnerable by underinvesting in systems? Had he pushed for too much, too fast?

Into the Breach

By day's end, Brett had assembled the top management team to review the crisis plan. Things seemed even more grim than they had in the morning.

Laurie informed the team that, with new information from additional banks, the number of accounts known to be compromised was increasing. The total was still not clear but certainly far more than the initial 1,500.

Sergei reported finding a hole—a disabled firewall that was supposed to be part of the wireless inventory-control system, which used real-time data from each transaction to trigger replenishment from the distribution center and automate reorders from suppliers. The system helped keep inventories low, shelves full, and costs and lost sales to a minimum. With the firewall disabled, however, supposedly internal company data were essentially being broadcast.

"All you'd need is the right equipment and the wrong motives," Sergei admitted. "But you'd have to be somewhere relatively close to the store because the broadcast range is limited." He paused to survey the expressions of his colleagues, ending with Brett. "We can get the firewall back up as soon as the cops give us the go-ahead." He knew his job was on the line.

"How did the firewall get *down* in the first place?" Laurie snapped.

"Impossible to say," said Sergei resolutely. "It could have been deliberate or accidental. The system is relatively new, so we've had things turned off and on at various times as we've worked out the bugs. It was crashing a lot for a while. Firewalls can often be problematic."

Brett looked at the human resources director, Ben Friedman, who had several personnel folders in front of him. "We've had five departures of people who were involved with that system in some way," Ben said, thumbing through the files one by one. "Two resignations, one to return to grad school, one termination for a failed drug test, and one termination for downloading inappropriate material using company computers." He placed the folders on the table, paused, and slid the two for the terminated employees over to Brett.

"Well," Brett sighed, "that gives us a couple of possible suspects." He turned to the communications director, Sally O'Connor. Earlier that day, she had handed Brett a memo outlining three communications options, which Brett had been contemplating ever since. Holding a press conference would get Flayton's out in front of the story—and it would, Brett thought, be the most forthright approach. He was troubled by Sally's second option—informing customers, by letter, that there had been a breach and that the situation was being addressed. He felt it might generate more customer anxiety than reassurance and could make Flayton's appear to be hiding something. The final option—do nothing until law enforcement was ready to go public—was the easiest in the short term because it put the decision in other hands.

Darrell Huntington, longtime outside counsel for Flayton's who had been briefed late the previous night, rose from his seat. "Let me say a couple of things. First, we still have no definitive proof here. All the evidence is circumstantial. And from my review of past cases, it's clear that whoever goes public first is the entity that gets sued."

"Who would be most likely to bring the suit?" asked CFO Frank Ardito. "No customer will suffer financial damage, right? The banks protect them."

"We could be sued on any number of grounds I won't go into here," said Darrell, "but other breaches have brought lawsuits from customers, banks, and even investors.

Whether you win or lose, it costs you—and there's bound to be a lot of media coverage."

"Aren't we required to disclose this to our customers immediately?" Frank inquired.

"Three of the states in which you operate require immediate disclosure, and the other three do not," Darrell noted. "But from what I understand, you don't know what role, if any, Flayton's has in this possible crime. A bank has identified a pattern. There seems to be a correlation between cards with fraudulent activity and cards used to make purchases at Flayton's. That could be a coincidence. At this time, we have no actual evidence of a data breach at Flayton's. None."

"What are we supposed to do?" Brett pressed. "Doing nothing is not an option. Not for me."

"That is exactly what you *should* do," Darrell asserted. He turned to Sally. "Your communication strategy should be not to talk to anyone. If you do get a call from the media, simply confirm that Flayton's has been contacted by law enforcement authorities regarding an investigation about which you have been given no information and with which you are cooperating fully. Refer them to the Secret Service. They don't tell anybody anything."

"That may work for now," Brett acknowledged, "but, Sally, I want you to anticipate the next steps. However we communicate eventually, I want to offer straight talk, not spin." Darrell sat down.

Brett knew there were no easy answers. His online search last night had turned up a recent survey documenting that customers are reluctant to shop in stores known to have data breaches. Darrell was arguing that Flayton's could be vulnerable simply by trying to do the right thing and getting the news out quickly. Yet, the company's future depended on its reputation for fairness—one painstakingly earned over decades by Brett's father.

"Well, the decision may soon be out of our hands," said Sally. "I was reviewing the affected accounts, and one very interesting name cropped up: Dave Stevens, evening news anchor at KCDK-TV. Apparently, we installed a home theater for him." She turned to Brett. "Stories like this always leak somehow."

Brett shifted his jaw, pushed back his chair, and stood. "So if I understand this correctly, we have circumstantial but strong evidence that a breach has occurred, we have two former employees who might or might not be involved, some states that require we disclose, feds who want us to shut up, and a television personality among the victims. If we disclose, we'll probably get sued; if we don't, the story will eventually leak. The feds may get the perpetrators if we give them time, but there's no guarantee. No matter what, our reputation is on the line, and competitors will start running promotional specials to lure customers away first chance they get. And I am wondering if I can ever look a customer squarely in the eye again. Did I miss anything?"

Brett leaned forward and put both hands firmly on the table. His eyes met those of each member of his team. He knew—and trusted—them all. "The one thing I'm sure of is this: The Flayton name means something to me, to our employees, and to our customers. We're going to decide what to do. Today."

How should the Flayton Electronics team respond to the crisis? • Four commentators offer expert advice.

See Case Commentary

Case Commentary

by James E. Lee

How should the Flayton Electronics team respond to the crisis?

How you react to news of a security breach at your company is, as a practical matter, much more important than what actually happened. Whether your business can survive the episode will depend on the corrective action you take and how you communicate about it to the various stakeholders. My firm's experience offers an excellent illustration.

ChoicePoint provides decision-making insight to businesses and government through the identification, retrieval, storage, analysis, and delivery of data about individuals and institutions. In 2005 our company was the victim of a fraud scheme in which criminals posed as customers to obtain the personal information of 145,000 people from our data systems. No technology breach occurred, but the media characterized the incident as if one had. We discovered the nefarious activities ourselves and reported them to the Los Angeles County Sheriff's Department, with whom we set up a sting operation that eventually led to the prosecution of a Nigerian crime ring.

Beyond fixing the firm's weaknesses in data security, the CEO must develop a brand-restoration strategy.

We agonized over choosing the right strategy for alerting consumers whose data may have been obtained fraudulently from ChoicePoint. In the end, we notified everyone believed to be at risk, regardless of their state of residence. We updated employees daily, and we had frequent conference calls with managers and officers. Our CEO and other senior executives visited key customers and investors to share the many new policies and procedures we were adopting to prevent a recurrence. All of these stakeholders were, we recognized, pivotal to our survival.

Some of our preventive steps were radical, including abandoning a line of business worth $20 million because of its potential to risk a future data breach. Changes in culture often were required. For example, every employee must now pass yearly privacy and security training courses as a condition of employment.

At ChoicePoint, we learned quickly that in situations like these, many factors are beyond your control. The media can be a huge distraction. But it's much worse than that. You face inquiries from many quarters, in our case from multiple state attorneys general, the Federal Trade Commission, and the U.S. Congress. You might be sued by banks; by others involved in the credit card transaction chain, such as processing companies and consumers; by shareholders; and even by employees and retirees.

For Flayton Electronics, moving swiftly in the face of crisis will be essential. Timing is a crucial factor in the inevitable lawsuits, which focus on what executives knew and how long they knew it before going public. Beyond fixing the firm's weaknesses in data security, CEO Brett Flayton must develop a brand-restoration strategy. The company should, as ChoicePoint did, notify the affected customers rapidly, set up toll-free information hotlines, and offer credit-monitoring services. Then they must exceed these basics with a broad range of extras to keep customers loyal: Offer discounts and sales, meet with critics of the company, and develop and promote new web pages that outline reforms in the firm's policies and practices.

Communiqués will also need to evolve to demonstrate responsiveness to developments, or else risk that the words of company executives will be perceived as just corporate lip service. Tone is very important. Public statements must be not only accurate, but sincere, contrite, and honest.

Flayton's will also have to address the influence of blogs, viral videos, and other social media. Such user-generated content, unfiltered by traditional journalists and accessible by anyone using an online search engine, is often a mode of recruiting lawsuit plaintiffs and airing personal grievances.

Finally, Brett and his team will need patience in spades. The problem will not go away when the headlines do. Mitigating the effects on brand and reputation will take, I estimate, three to five years. Flayton's has a long road ahead.

James E. Lee (james.lee@choicepoint.com) is the senior vice president and chief public and consumer affairs officer at ChoicePoint, based in Alpharetta, Georgia.

Case Commentary

by Bill Boni

How should the Flayton Electronics team respond to the crisis?

Most senior executives have the insight and the measurement tools to assess potential damage from tangible disasters such as floods and fires. That's not often the case when it comes to information security, including prevention of and planning for data theft. "Let the technical staff handle that" tends to be the default strategy, with responsibility relegated to nonsenior IT or corporate-security management. Businesses that are serious about protecting their data and preserving the data's value should have a high-level official, such as a director or a vice president of information protection, who serves not merely as a manager but as a senior champion in this area.

Seven years ago, I was appointed Motorola's first-ever corporate information security officer. As a data-protection leader, I am responsible for the firm's information and IT environment globally and for having a comprehensive strategy for risk management. One useful strategy component is to require every new initiative to identify, in the initial idea phase, the data that might be involved—and their value. This mandate builds appropriate safeguards right into the projects themselves. Also beneficial are policies, procedures, and training protocols that are customized for each company function, to reduce the likelihood that individuals will make wrong choices because they do not understand how the overall data standards apply to their specific roles.

You need people on hand with the digital expertise to match wits with tech-savvy cyber criminals.

Being fully PCI compliant is, of course, a vital first line of defense against data theft, and my best guess is that a third of companies meet that standard. However, increasingly capable cyber adversaries do not give up and offer their congratulations because you did what you were supposed to do. During my tenure in information security, hobbyist hacking has evolved to become a much more sophisticated, parasitic extraction of valuable data from targeted organizations. One common fallacy is that silver bullet technology can save the day. I've seen organizations spend hundreds of millions of dollars on security safeguards that were penetrated by a knowledgeable person with a handheld device. For example, Motorola proved to one of its customers, who had invested heavily in some of the best protection technology available, that we could access their core business systems using just a smartphone and the Internet.

To prevent and cope with data breaches, you need people on hand with the digital expertise to match wits with tech-savvy cyber criminals and to understand the systems they're targeting. Data protection isn't necessarily a core competency of either an IT or a traditional loss-prevention team. Also indispensable are knowledge of the applicable privacy statutes and regulations, and the ability to gather and preserve sources of relevant evidence. You can assemble an internal team of lawyers, accountants, and experienced digital-forensic investigators from law enforcement or defense agencies—or use external sources such as law firms, public accounting firms, and consultancies with digital specialization.

Armed with facts from experts, yet to be assembled, Flayton's should put law enforcement on notice that the company exists to serve customers and maintain its reputation. Flayton's can't afford to wait indefinitely to inform the public. The firm should, of course, work with the Secret Service to achieve prosecutions but must also make it a priority to maintain the public's trust while complying fully with data-protection and privacy laws in states that require breach disclosure.

Until Flayton's thoroughly understands its security status, it risks making poor choices. None of the managers or advisers appears to have enough experience or information to reach sound decisions about the risks they are confronting. For example, allowing the firewall to remain down may compromise even more customer accounts. An established model response plan, such as that from the American Institute of Certified Public Accountants, is one potential source of immediate help for this company in crisis.

Bill Boni (bill.boni@motorola.com) is the corporate information security officer for Motorola in Schaumburg, Illinois. He is also a vice president and board member of the Information Systems Audit and Control Association, a global organization based in Rolling Meadows, Illinois.

Case Commentary

by John Philip Coghlan

How should the Flayton Electronics team respond to the crisis?

A data breach can put an executive in an exceedingly complex situation, where he must negotiate the often divergent interests of multiple stakeholders. Witness the array of players you would encounter in a case like that of Flayton Electronics.

Banks that issue payment cards, such as the fictional Union Century, are often the first to spot possible fraud when their systems identify merchants who are common points of purchase for potentially compromised accounts. For the protection of their cardholders, they strongly support early identification of these merchants.

A bank that performs payment processing for a given merchant, called the acquiring bank, is protective of that business relationship and sensitive to the merchant's interests. However, that bank is responsible to payment networks such as Visa and MasterCard for certifying merchant compliance with payment card industry standards. Therefore, the acquiring bank's brand and reputation also are potentially threatened, and its interests are only partly aligned with those of the merchant.

Further complicating the situation is the role of law enforcement. The Secret Service has asked Flayton Electronics not to disclose the breach, believing that leaving the system vulnerability in place during surveillance provides the best chance to catch the thieves should they act again. Unfortunately, such requests can be open-ended, and with each passing day the opportunity for the company to lead in communications is frittered away. It is not illegal to refuse such appeals from law enforcement. On the contrary, many state laws require a breached entity to disclose specific information in a timely way.

Beyond the institutional stakeholders just described, there are consumer groups, legislators, shareholders, and of course the employees and customers, whose interests we see Brett Flayton actively considering. Regarding customers, the CEO might wish to know that in a study by Javelin Strategy & Research, 78% of consumers said they'd be unlikely to continue shopping at a store once they had learned of a data breach there.

So our harried CEO has no better option than disclosure. If he doesn't speak out, he is not allowing his customers the best means of protecting themselves: by using a different, uncompromised payment card or by scrutinizing transactions on the compromised card. Even if he waits to learn more, Brett will eventually have to go public, still lacking complete information. In the meantime, he runs a rapidly escalating risk that another party will disclose the breach, at which point he will need to defend having violated his customers' trust. The electronics firm has built its reputation on honesty, a fact that Brett and his advisers should not let each other forget.

So Flayton Electronics must communicate—right now—with its customers. Among the potential avenues are to use contact information from the store's own database; to set up a special company web page; and to hold exclusive informational events, such as call-ins and webcasts—all reinforced with a customer support hotline.

Of course, Brett should make sure that Sergei addresses the known technological weakness immediately. Customers will want to know when the system is safe again. Making data security a priority for the future—and communicating the specific policy changes that flow from that—may allow the company to become recognized as a leader in this area.

Research from Bain & Company also offers some hope: Customers who receive adequate compensation after making a complaint are actually more loyal than are those without complaints. So, if Brett Flayton's company provides a timely, focused, and effective response, his compromised customers might just become the most loyal of all.

Making data security a priority for the future—and communicating the specific policy changes that flow from that—may allow the company to become recognized as a leader in this area.

John Philip Coghlan is a former president and CEO of Visa USA, headquartered in San Francisco.

Case Commentary

by Jay Foley

How should the Flayton Electronics team respond to the crisis?

The executives at Flayton Electronics are being misinformed by Darrell Huntington, their outside counsel. The companies that get sued are not those that are first to go public about a data breach but those that do so poorly. Right now, Flayton's has no chance of putting out good information, because it doesn't have any. Announcing inaccurate information and then having to correct it as the breach investigation evolves would encourage a feeding frenzy of plaintiffs' lawyers. For now, Flayton's should remain quiet, but for reasons different from Darrell's.

Not alerting customers right away is not the same as doing nothing.

Another misconception of the management team at Flayton's is that they should consider notifying customers themselves. The credit card transactions belong to a bank that has protections in place for its cardholders. For Flayton's to mire itself in identifying private addresses for—and then contacting—potentially affected individuals would be to expose itself to liability. Someone else in the transaction chain, such as the credit card processing company, might very well be at fault, in which case it would be wise to wait for that party to come forward first. In fact, it is possible that the Secret Service investigation will show that the electronics retailer was not the source of the breach at all.

Law enforcement officials have asked Flayton's to remain tight-lipped while they do their work, to give them a better chance of apprehending the criminals. If Flayton's rushes into a public announcement, the bad guys have the chance to disappear, only to resurface elsewhere. Nothing positive will have been achieved with that result.

Instead, CEO Brett Flayton should calmly think through his crisis response. Not alerting customers is not the same as doing nothing. The company's first action should be to reduce the risk for future thefts by closing any data-transaction loopholes that this incident has brought to light, provided that the Secret Service does not think it will interfere with their investigation. The executives at Flayton's should also reevaluate their internal policies and procedures, and should establish regular self-audits and strategic-planning assessments. Sergei, the CIO, really fell down on the job. There's no excuse for his sloppiness.

Sadly, though, Sergei's technological woes are not unique. In 2006 the Computer Security Institute in San Francisco conducted a survey of 616 large, U.S.-based companies and found that 52% had experienced some kind of unauthorized use of their computer systems. Almost half of that subset said they suffered a laptop or mobile device theft.

Unfortunately, the true scope of the data-theft problem is not known. Hard statistics on its long-term impact, whether for companies or individuals, are scarce. From the Computer Security Institute, we have the figure that only 15% of their surveyed companies suffered financial losses as a result of cyber security breaches. We also know that most victims of data theft do not then become victims of identity theft. Typically, a criminal is out to rack up a few quick purchases using stolen credit cards and then move on. In fact, it's likely that customers at Flayton's were victims of this type of fraud. Thieves might reasonably assume that people who have money to buy fancy electronics have enough disposable income not to notice extra charges on their accounts immediately.

Perhaps the most worrying indicator is that the criminal industry for information is growing. I can go to MacArthur Park in Los Angeles any day of the week and get $50 in exchange for a name, social security number, and date of birth. If I bring a longer list of names and details, I walk away a wealthy man. This gritty new reality illustrates how much the value of personal data is increasing and should encourage every company to take data protection very seriously.

Jay Foley (jfoley@idtheftcenter.org) is the executive director of the Identity Theft Resource Center in San Diego.

Reprint R0709A
Case only R0709X
Commentary only R0709Z
To order, call 800-988-0886
or 617-783-7500 or go to www.hbrreprints.org

To Order

For *Harvard Business Review* reprints and subscriptions, call 800-988-0886 or 617-783-7500. Go to www.hbrreprints.org

For customized and quantity orders of *Harvard Business Review* article reprints, call 617-783-7626, or e-mai customizations@hbsp.harvard.edu

Harvard Business Review
www.hbrreprints.org

U.S. and Canada
800-988-0886
617-783-7500
617-783-7555 fax