CUSTOMER AWARENESS OR CUSTOMER BEWARE?

DATA SECURITY IN A CRM-OBSESSED INDUSTRY.

by Elizabeth L. Ivey

I may or may not be *your* ideal customer: A fairly frequent business traveler and avid vacationer, willing to pay more for better service, to behave loyally when impressed and to positively influence others through word-of-mouth advertising. Seldom do I search for the lowest rate available and I am likely to use a lower cost distribution channel when making my reservation.

So, would you like to know me better? How much information are you capable of collecting in an effort to anticipate my needs? How much information will I volunteer myself and how much will you uncover without my awareness? Will your methods of data acquisition give me the shivers?

In a crusade to understand customers better, there is always a risk of repelling them. Yet when a hotel employee pulls off something extraordinary with carefully timed intuition, the results can be profound. Will your hotel be rewarded with return visits for repeatable acts of superior service? It is highly probable. But equally important to this successful CRM equation is how well you can protect guest privacy and secure individual identity.

Pervasive Personal Recognition

Yes, you think you'd like to know me better. I've stayed at your property numerous times so what do you know about me? I stayed two weeks at one of *your* properties, how could you *not* know that about me? Can I trust you with this knowledge? Who has access to my data and how will it be used?

Although a typical customer is unlikely to ask the above questions, consumers are increasingly concerned with security and confidentiality. Just 42 percent of consumers think businesses handle personal information in a proper and confidential way.[1] Customers who are worth keeping may begin asking more straightforward questions about their privacy vis-à-vis your CRM initiative. Be prepared to answer them with a policy and enforced practices.

Fear Factor

It's not my style to breed fear or mistrust so I will spare you the alarming trends of credit card fraud and identity theft. Perhaps more relevant is Gartner's estimate that by 2005, 1-in-5 enterprises will experience a serious attack that results in a material loss for the company. Repairing that damage will far exceed the cost of preventative measures. Litigation and restitution are likely to result, along with prolonged negative impact on public perception.

Security specialists strongly warn *all* businesses (from enterprises to proprietorships), "If you don't protect yourself you're going to experience an attack." Not because your data is the most lucrative or because some cyberpunk has something against your company, but simply because your data management infrastructure is virtually undefended.

When it comes to information security in the hospitality industry, there are few standards and little expertise. Hospitality IT professionals are not willing to talk publicly about the *lack* of attention paid by the entire industry to this increasingly important matter. Unfortunately, hackers are all too willing to share news of security vulnerabilities and exploits.

A Higher Level of Obligation?

Not surprisingly, regulated industries (gaming, finance, transportation and healthcare) do a better job of protecting themselves from security breaches. Many industries are governed by legal requirements for protecting data. The Gramm-Leach-Bliley (GLB) Act sets rules for the financial services industry, and the Health Insurance Portability and Accountability Act (HIPAA) monitors healthcare companies and benefits providers. Almost any company doing business over-

seas may have to follow rules established in other countries, such as the European Union's Directive on Data Protection.

Whether you manage information for a global chain, an intimate boutique or a family lodge, you need to worry *fiercely* about protecting customer data. It should be no surprise to hoteliers that names, addresses, credit card and bank card information are classified as highly sensitive in the banking industry. If you are capturing divulging details about your guests' behaviors and preferences, perhaps there is a higher obligation to keep that information out of the wrong hands.

"Major corporations and gaming operations are able to put significantly more energy into defending against malicious attacks. Hackers are drawn to places that are easiest to penetrate and the most poorly defended," said Glenn Bonner, CIO of MGM MIRAGE. Bonner agreed that (unfortunately) it might take an ugly instance of privacy law violation in the hospitality industry to underline the importance of protecting customer data. Almost inevitable is legislation to protect guest data as stringently as financial transactions and medical history. (See "Comments on the California Civil Code" on page 126.)

Also of increasing concern is whether companies can be held liable for having inadequate security. Experts fear stylized personal injury lawsuits filed by customers whose personal information has been disclosed, corporate lawsuits based on damage caused by security breaches between business partners, and even class-action lawsuits filed on behalf of jilted stockholders.[2]

Foresight Is Inexpensive So Get a Plan

If you didn't budget a dime to spend on technology projects this year, you are not relieved of your duty to protect existing IT investments and customer assets. There is increased awareness of the vulnerability of the hotel industry, but don't wait for legislation to tackle it. Many of the federal regulatory acts governing other industries require a written information security plan. Proactively creating such a plan, long before legislation mandates it, will give you a foundation from which future security initiatives should be launched. A comprehensive plan to safeguard customer data addresses the administrative, technical and physical levels of security.

Certain security mechanisms may be built into hospitality business applications to prevent accidental, unauthorized access to data; however, more sophisticated types of security, such as encryption, usually are arranged for separately. Almost all safeguards, such as firewalls and intrusion detection systems, are the responsibility of the hotel or hotel company, *not* the application vendor. Nor is security the domain of the hardware installer, although a large part of security involves protecting the servers on which the applications and data reside.

In addition to deterrent systems and preventative measures, detection systems have enormous value in ongoing security initiatives. Detection software watches for unauthorized activity on a system by identifying, reporting and even responding to suspicious activity. Less than half of companies have intrusion detection systems in place.[3] Without one, it is difficult to know exactly what kind of threats you may be facing.

Tom Murphy, CIO of Royal Caribbean Cruise Lines (RCCL), was astonished to learn that his intrusion detection system has registered no fewer than 500,000 attempts to compromise the RCCL network since the beginning of this year. That number includes viruses sent via e-mail, Web service probes and other malicious acts. While initially hard for Murphy to swallow, the ROI findings might conclude that 500,000 threats were thwarted or pin-pointed by a solid security investment.

Who Secures the Customer Data?

A reasonable amount of energy and expense should be put into assuring that data doesn't leave the premises, but what happens when customer data must pass from one entity to another? This might include distribution providers, channel managers, Web application developers, technical support services and transaction processors. Be aware of your business partners' security practices. When sharing customer information with them, hotel companies need to know that it's protected. Poor security practices of others could become a liability.

A few years ago, a wild debate raged over customer data. Franchisors, property owners, management and distribution companies claimed it as their own. In many cases it was clear who won the birthright to customer data, but does that make one entity solely responsible for its well being? Data owners usually assume certain responsibilities, but how can a brand or distribution partner be responsible for safeguarding the data at the property level? A growing number believe that data security definitions and requirements need to be written into all franchise and management contract agreements, along with appropriately projected investment levels and technical guidelines if necessary.

Make a Plan

The best defense is to get your company talking about security, acknowledging that something could go dreadfully wrong. All good security initiatives begin with a thorough risk assessment. Policies and procedures are then developed or modified to mitigate the risks. Documentation should include guidelines for classifying customer information and for backing up databases. Management of key vendor relationships should also be addressed. The plan should include actionable tasks for ensuring the integrity of customer data.

Attempting to calculate the ROI on a major security project is highly fallible. The costs of safeguarding customer data should not fall prey to traditional metrics and should nearly transcend budget scrutiny. It is estimated that 1-in-3 companies would lose critical data or operational capability during a disaster because their recovery plans are not adequately funded.[4]

In addition to approving investments in IT security initiatives, senior executives must establish a corporate culture that endorses security. A warmly phrased privacy policy is not sufficient. A safeguarding policy describes the processes that protect customer information from unauthorized access. Senior executives and the board of directors should be presented with the safeguarding policy for explicit approval and to ensure accountability.

While every type of organization is under pressure to protect its network, safeguarding customer data is not the responsibility of "the IT guy" nor is it a purely IT function. It is up to the company, not the technology decision maker, to determine the value of the customer data, the perils of Internet commerce and how much trust is too much.

Elizabeth L. Ivey is a senior technology strategist with HVS International, a global hospitality consulting firm. She can be reached at (303) 443-3933 ext. 220 or eivey@hvsit.com.

Notes

[1] *Harris Interactive Poll, March 28, 2003.*
[2] *Scott Berinato and Sarah Scalet, The ABCs of Security, www.cio.com, February 20, 2002.*
[3] *Top Layer Networks, 2002 Survey of Security Experts, February 27, 2003.*
[4] *John Surmacz, Cash Crisis, www.cio.com, March 12, 2003.*