

# KNOW YOUR CLIENT



Customer education isn't a one-size-fits-all practice. It must be tailored for the individual, reports **Frank Washkuch**.

**A**sk any IT expert for a cookie cutter approach to protect customer data and there might not be much of an answer. After all, hackers are just one group to worry about when looking to prevent the theft of customers' personal information. Company executives also must concern themselves with their own employees, as well as government legislators.

This is because secure ecommerce is not only about understanding and foiling a multitude of internet threats, but also adhering to state and federal legislation in addition to protecting against insider threats.

Spearheading an effective all-around strategy that maintains secure commerce for customers therefore means first outlining all the risks — otherwise such a process could become chaotic.

"You'll get buried pretty quickly," says David Grant, vice president of marketing for Watchfire, a web applica-

# Safeguarding the consumer

tion security vendor. “You have to go out and find customers’ security vulnerabilities first. Generally speaking, there’ll be a ton of them.”

## Determine your goal

An early decision in the process of implementing a security solution occurs when companies decide what kind of security features — and how many or how few — they want to protect their home users. While it’s certainly possible for a company in the financial or health care sectors to employ dozens of security features on a website accessible to home users, firms must determine how much of those security features will impact their website’s usability.

In short, firms must ask if they’re creating a website security strategy that is burdensome for home users, says Jaime Chanaga, chairman and CEO of The CSO Board, a management consultancy firm.

“I think what’s happened is that in many industries like financial services, there’s only so much you can do with the technology. You can make it as difficult as possible to log into a site. The user could have to answer 20 different questions. I think what a lot of organizations are starting to do, and where they’re starting to focus a lot of their efforts, is not on the technological applications used,” he says. “A lot of them are saying, ‘Are we really going to deploy \$50 million in security for one transaction looking at cancelled checks?’ What banks and other organizations are doing is they’re really focusing on a risk-based view of security for their online presence, not the specific technology, but how you the customer dial into the risk.”

Once corporate officers are filled in on the benefits of a security strategy, the onus falls to them to educate employees and customers. One way companies can help themselves is by using their human resource and privacy department as an advantage, says Chanaga.



**A year ago, insider threats were a rare thought. Now it’s at the forefront.”**

— **Brian Contos**, CSO, ArcSight

“Usually in most organizations, a lot of the end-user training comes from the chief privacy officer or an officer from the CPO’s office. There are a couple of reasons for this, because we’re talking about customer privacy issues driven by the *Health Insurance Portability and Accountability Act of 1996 (HIPAA)* or the regulations in California [*California Senate Bill 1386*, also known as the *Security Breach Information Act*], for instance,” he says. “We’re starting to see a lot of human resource departments become very savvy about the training they give their workforces on privacy and security. That’s a good thing — you need a system of checks and balances.”

## Develop a lesson plan

Mapping the latest threats from both the inside and outside is one way to begin developing such a system. This means companies must undergo a risk assessment evaluation before even beginning to work with experts on expanding their IT security knowledge.

A company’s understanding of its security landscape determines how much more education its employees need, says Grant. “With the lower half [of customers], there are ones that need a lot of hand-holding. For them we have an on-demand software and we do scanning and testing remotely,” he says. “There are also people who have been doing this for a while. For us, that’s more about checking security along the way and helping



them develop self-practices.”

Before educating customers on various security risks, it’s also critical to gauge the levels of access of employees serving the public, says Chris Young, senior vice president and general manager of RSA’s Consumer Services Division.

“One size does not fit all as far as how you apply different types of security to different user populations. Most consumer-facing businesses have consumers, inside users and different user populations with very different needs,” he says. “Different levels of risk live in different user populations depending on what information they have access to. The level of risk is different, so it does require some thought given to the differences in populations. You need to understand what level of security each population requires, and also what type of security is going to work for that population.”

## Multi-factor authentication

One complicated lesson is how financial firms can keep their businesses compliant with existing authentication standards, as well as preparing for impending regulations to take effect in coming months.

Understanding of Federal Financial Institutions Examination Council (FFIEC) guidelines has increased in recent years — even in boardroom level positions, according to Young. A result has been a marked increase in the use of verification methods to ensure banks are dealing with proper users, and that con-

# Safeguarding the consumer

sumers aren't mistakenly entering personal information onto malicious websites.

"I haven't run across a lot of organizations that have absolutely no idea what they need to do to be compliant with the FFIEC. In a lot of cases, FFIEC compliance is directly relevant to what we're trying to do, so the questions are more along how or when or how much.

They're not struggling to understand what they need to do," he says.

"[Security education among financial institutions] is constantly improving. With one very large global bank, I know that this is visible at the board level with them. There's a lot of interest, and most organizations have teams of people and cross-functional groups engaged."

International firms have the additional onus of ensuring their practices are in line with the regulations of multiple countries they do business in, says Andrew Krcik, vice president of marketing for PG, a leader in encryption and digital-signature solutions.

"Germany's requirements are very different from the U.S. You have to be aware of what the requirements are around the world," he says.

## Know the inside threat

Companies are also gleaning information on one threat they can't just buy a technological solution to solve. Insider threats are a growing concern to many firms, which want to know what they can do to keep careless employees — or those with malicious intent — from disclosing valuable company-held information.

And if a news of a data breach goes public, companies can be exposed to embarrassment and loss of consumer confidence, on top of having to launch an investigation into who might be in possession of the compromised data.

While company knowledge of insider threats has improved, many firms are still scurrying to educate their employees on how to avoid carelessly disclosing data, according to Brian Contos, chief security officer at ArcSight, a global leader in enterprise security management (ESM).

"I think it really has improved. If I was talking to a corporation a year ago, insider threats were a rare thought — now it's at the forefront," he says. "At the end of the day, people understand that insider threats are a problem, that these aren't things related to some nameless hacker on the other side of the ocean. These are trusted employees."

When trying to prevent the loss of personally identifiable information, firms should emphasize proper personal behavior, since many data breaches are the result of carelessness.

But education of employees can help to keep a loss of customer information — and unwanted media attention — at bay, says Fred Rica, partner in PricewaterhouseCoopers' technology risk services group.

"If there's a problem, a lot of security and ID security is behavior-based. A lot of people don't shred documents for instance," he says. "Probably the hardest thing to do is to raise people's awareness. Technology will only get you so far. That might get you 90 percent of the way there. But you have to get people to think about their behavior."

## Power of the pocketbook

Customers themselves are realizing they have a direct influence on firms' security policies and even the techniques they employ.

Thus, educating personnel is also becoming easier for firms because of

## STILL SCARED: Customer worries

**44%** of Americans think their information is safe when engaging in ecommerce.

**50%** avoid making purchases online out of fear that their personal information will be stolen.

**34%** feel that online banking is as safe as seeing a teller in their neighborhood bank.

**24%** feel that corporations are placing the right emphasis on protecting information systems and networks.

Source: Cyber Security Industry Alliance, May 2006

media attention on security events and lapses in compliance. These are some of the "few factors driving the perfect storm [toward security awareness]," says Rica.

"There's a lot of pressure coming from the consumers, then you've got a slew of legislation and regulation that's come out over the past four to five years. Put those two together, and you have a company thinking that if it doesn't do this stuff well, it could really cost them money," he says.

"The other part is the shareholders screaming that they don't want to have to pay tens of billions of dollars in fines. I think that's an enormous influence. Anytime you have regulations with those types of fines, it gets people's attention." ■

*We welcome your comments. Email us at [sfeedbackUS@haymarketmedia.com](mailto:sfeedbackUS@haymarketmedia.com).*



## ArcSight, Inc

5 Results Way, Cupertino, CA 95014 • (408) 864 2600

ArcSight, a leader in Enterprise Security Management, provides solutions that serve as the mission control center for real-time threat management, compliance reporting and automated network response. By comprehensively collecting, analyzing and managing security data, ArcSight solutions centrally manage and mitigate information risk for security, insider threat and compliance. ArcSight's customer base includes leading global enterprises, government agencies and MSSPs.