Proven. Trusted.

TECH BRIEF: FINANCE
DATA PRIVACY AFTER SNOWDEN AND TARGET: IMPLICATIONS FOR CREDIT UNIONS

BY STEPHEN COBB, SENIOR SECURITY RESEARCHER, ESET

The cost benefits of transitioning members' banking activity to the digital channel are well known. The more banking that members do electronically—via website, email or text message—the better the bottom line for their financial institution of choice. But what if members stop trusting the technology? How would your organization react if online banking became less appealing? And what can you do to reassure members who may be feeling skittish about the Internet and email?

Before providing some answers to these questions, we must first consider what evidence there is that consumers are feeling skittish about technology. Is there any reason to think that widespread media coverage of large-scale electronic spying by the National Security Agency (NSA), exposed by former government contractor Edward Snowden, has spooked the public? Yes, there is.

A few months ago ESET commissioned a survey that asked adult Internet users if, based on what they had learned about government surveillance from the Snowden revelations, they agreed with the three statements listed below:

1. I am less inclined to use email.
2. I have done less shopping online.
3. I have done less banking online.

Nineteen percent of respondents agreed that they had done less online banking and were less inclined to use email. Fourteen percent admitted to having done less shopping online. You might see these results as good news—that the majority of Americans had not changed their online banking habits. However, when one in five users cuts back on something that is a vital part of your business model, you should probably pay attention, especially considering there were even more revelations of Internet-based spying by the NSA after our survey was conducted.

> "When one in five users cuts back on something that is a vital part of your business model, you should probably pay attention."

The Snowden effect

In November 2013, the Washington Post asked a large sample of Americans this question: "Since the revelations about the NSA have you personally taken any actions to better protect your privacy?" A quarter of respondents said they had. In other words, several sources point to a "Snowden effect" that is causing consumers to change their online behavior in ways that could undermine your ability to realize the full benefits and cost savings of electronic banking.

This changing behavior reflects a broader erosion of trust in the Internet and the companies that make it possible, driven by headlines about their cooperation with secret government surveillance programs. For example, when we asked people if they were now less trusting of technology companies such as Internet service providers and software companies, 50 percent agreed and just 44 percent disagreed (6 percent were undecided).

On the other hand, 74 percent of those surveyed said they would "admire a company that took a stand against unlimited government access to my personal information."

Consider another survey, this one from 1999, when the Wall Street Journal and NBC asked 2,000 adult Americans what they feared most in the coming century. Topping the list was "loss of personal privacy," which 29 percent of respondents said was their number one concern, well ahead of overpopulation, acts of terrorism and racism. While those concerns might have shifted after 9/11, there can be little doubt that privacy is again top-of-mind for many of your members.

> "Now is a great time to tell your institution's privacy story and highlight the ways in which you honor the privacy wishes of your members."

Talk to your credit union members

What does all this mean for credit unions? For example, should they become vocal critics of the NSA? Not necessarily. If your members are mainly federal and military personnel, you might find they weigh the benefits of surveillance versus loss of privacy differently from the general population. But it might not hurt to back broad calls for surveillance reforms, such as those proposed by tech companies in their open letter to the government (see reformgovernmentsurveillance.com).

However, the real value of understanding that your members could be feeling jumpy about data privacy these days is the opportunity it provides you to engage with them on this topic and trumpet all of the privacy protections you offer. Of course, you may already be doing this in the wake of the Target security breach, the other big trust-eroding event of 2013.

But as we travel the country talking to the public about Internet security and data privacy, we get a strong sense that financial institutions could be doing more to reassure their members. For example, there is confusion about the relative "safety" of debit and credit cards and a surprising lack of knowledge about the anti-fraud tactics that many credit unions employ (to great success in our experience).

Privacy—a continuing concern

Now is a great time to tell your institution's privacy story and highlight the ways in which you honor the privacy wishes of your members and protect their data. These days, it is no secret that fraudsters and cyber criminals are out there, looking to grab personal data however they can, so address the topic head-on. Have "the privacy conversation" with new and existing members, and you may find that it deepens the relationship and even prolongs it. After all, while events like Target and Snowden come and go, privacy remains a fairly constant concern for Americans, making this strategy a good long-term investment for your organization.

In the Washington Post poll, 69 percent said they were concerned about the collection and use of their personal information, whether it was by the government, phone companies or websites. The survey did not ask about banking. But how significant would it be if a future survey showed that credit unions were more trusted on data privacy than other financial institutions, thanks to their proactive engagement of members on this issue?