The One Control

I wanted to write about a very important subject. But I didn't know what to call this very important subject!

If you've experienced any of my workshops or webinars, you already know I believe in one primary control that trumps all others. The lowest hanging fruit, the key that locks the door, "The One Control" is … (drum roll please) …

Well, before I answer that, let me clue you in on how I prepared this article. First, I called a few friends to see if they'd offer some suggestions about The One Control. As information security officers (ISOs) of their banks, they oversee budgets ranging from thousands to tens of thousands of dollars. But I would not have called them, had I not known they agreed with me about The One Control.

I found they not only did these ISOs buy into my The One Control philosophy, but they improved upon it. The master was outdone by the grasshopper … my clients had developed The One Control beyond my own expectations. (In other words, I learned a lot from these interviews!)

So now I am ready to share with you what I mean by The One Control. But that is not as easy as you'd think. I don't even know what to call The One Control anymore! Interestingly, Laurie Rees (vice president-education & training for the Indiana Bankers Association) and I have been struggling to find a good way to describe The One Control. In fact, in a moment of serendipity, I was just now interrupted in writing this paragraph to brainstorm with Bobbette Fagel, Infotex vice president and compliance consultant, and Laurie about this issue. After mulling through several ideas about what to call The One Control, we settled on switching the name from "The User Awareness Program" to "GLBA Information Security: Teaching Acceptable Use to Your Users."

Wow. Talk about going from a big mouthful to an even bigger mouthful! But in preparing for this workshop, we learned that banks refer to The One Control in many different ways: GLBA training, information security training, acceptable use training, computer training, information technology training, "the-training-the-examiner-wants-us-to-do-about-computers" training, and security awareness training (my favorite)!

Notice that every name for The One Control has the word "training" in it. However the friends I interviewed taught me something valuable: Training is only one component of The One Control. Even though everybody calls it "(fill-in-the-blank) training," most ISOs view The One Control as extending far beyond training.

"If it's just an informational thing, it's a waste of time," says T.J. Deckard of United Commerce Bank, Bloomington. "It's about establishing the right mindset."

I like that … mindset. I liked it so much, I considered naming this article, "The Mindset."

I asked T.J., who serves his bank as IT director, to explain what he meant by the mindset. "That's hard to answer," he said, "but I know that when I'm successful, it's because our users are shifting from a 'trust everyone' mindset to an 'ask questions' mindset."

Hmmm. That makes sense to me, especially since pretext calling is on the rise these days. The bad guys are calling and asking for information they are not supposed to have. Simply by asking for it, they are breaching security … often using the information they get to steal identities or leverage other attacks.

Unfortunately the user's desire to be polite instead of asking questions is damaging reputations. So the task for T.J. and other bank ISOs is to find ways to not only teach the acceptable use of computer systems, but to motivate employees to be on guard … to keep aware of the threats and vulnerabilities that they, the people controlling the information, face in everyday life.

Don Smith, the ISO of STAR Financial Bank, Fort Wayne, makes use of computer-based training, due to the large number of people he needs to reach. However he tries to get out in front of each and every employee at least once a year, and he sees benefits beyond the goal of user education. "Because our users are well-trained and have heightened awareness of ongoing issues, our customers and their families and friends are starting to view them as a reliable source for information about ongoing threats and scams."

Now that's excellent! The community is seeing the bank as a source of information about information security! And what Don and others I've interviewed understand is that this approach overcomes the politeness versus security problem.

This viewpoint is backed up by my two smallest clients. "We have the luxury of knowing, or at least attempting to know, all of our customers," says Patrick Duffey, president of State Bank of Burnettsville. But information security comes naturally to this bank: "Making eye contact with those we don't know, and politely offering to help them," says LaDinna Altman, the bank's IT officer, "is the best way to not only serve the customers, but scare away potential bad guys."

I love it when information security morphs into customer service. And I know that if I can help my clients teach their employees to stay ahead of ongoing threats and scams, in turn my clients will better serve their customers.

How do you get your employees to invest the time it takes to learn information security best practices? "What I try to do," explains Cindy Schrier, ISO of Home National Bank, Thorntown, "is mix the ongoing awareness information with tidbits that our employees can put to use in their own home computer systems."

In other words, personalize the training, and the users will value it. But doesn't that mean that The One Control is about ongoing threats and vulnerabilities, current reports in the paper or on the news, and not just best practices? According to Ralph Marcuccilli, chief information officer of STAR Financial Bank, "In order to keep employees vigilant, it is important to weed out the hoaxes, so they are not inundated with threat alerts. Assigning one person to the task of awareness helps filter the noise down to credible, high-priority information."

So the awareness proposition is about a process for filtering out the noise and keeping the team on their toes. "In that regard," advises Al Fullerton, assistant vice president of communications/IT security for First Bank Richmond, NA, "always be looking for actionable information in test results — from examiners, auditors, internal tests — that you can take back to your team in real time."

Now Al was speaking my language! (My firm does a lot of testing.)

"The main goal is to increase awareness through experience," says Fullerton, "not just information. But the tests don't have to be formal IT audits or assessments by third parties."

What? Tests without third parties?

“It’s as simple as doing periodic walkthroughs,” offers Doug Bell, systems and vendor manager for Indiana Bank and Trust Company, Columbus. Doug affixes a special little sticky note on unlocked file cabinets and other acceptable-use violations. (See sidebar.)

“It can be a fun thing,” says Gary Kern, CIO of Mutual Federal Savings Bank, Muncie. I decided to interview Gary when I saw an e-mail he sent to his users. The subject … “$100 for you — Free!” … helped introduce Gary’s monthly awareness reminder about social engineering. It caught my attention, it caught the attention of his users, and it made the point.

But Gary was one of many who cautioned against relying solely on the e-mail approach. Scott Mayes, certified information systems security professional of Indiana Bank and Trust Company, agrees: “E-mail is easy and free, and I use it a lot — but you have to interact directly with the users.” He adds: “It is critical that you help them think for themselves about the threats and vulnerabilities.”

Think for themselves? How do you do that? “I’ve found that if you ask the right questions,” says Scott, “the users will generally figure out the right answers for themselves.”

Now that’s awareness — the ability for users to effectively respond to threats and vulnerabilities without being told in advance exactly how to act. The One Control is really an entire set of creative, dynamic activities — a program of thoughtfully planned activities to lead users to think for themselves. I think that’s what T.J. Deckard means by changing the mindset.

Ahhh, now I get it … The User Awareness Mindset …

Hey, Laurie — can we change the name of that workshop again?

About the Author: Dan Hadaway, CISA, CISM

Dan has worked extensively with banks on policy issues, engaging on projects ranging from gap analysis to developing a full policy set for denovo banks. He can tailor his consulting to any size bank, working on simple user-level policies with banks as small as one location to overseeing the entire IT strategy for a publicly held company. He has provided management-level regulatory compliance training for Fortune 500 companies as well as user-level awareness training for the smallest of banks. His strength is helping banks decide where in the "security/compliance spectrum" they should be. He has helped develop risk management programs and processes for banks as large as 2.5 billion and as small as 26 million in assets.

*He is the Managing Partner of **infotex**, an Indiana Bankers Association Preferred Service Provider in several areas, including Information Security Training.*