The Lowest Hanging Fruit

First of all, I'm a purveyor of risk assessments for everything. As such, I want to admit right off that I don't believe in the whole "low hanging fruit" concept. In fact, I've been known to take rotten apples into workshops and speeches to make the point that all low hanging fruit does not necessarily deliver value.

It's ironic then, that I preach there is one thing you, as a security manager, can do to substantially mitigate risk without the benefit of a prior risk assessment. It's nothing new. It isn't rocket science, nor is it something that you need to spend a lot of time chasing certifications or going to college to pull off. But it is a powerful mitigating control.

It's Security Awareness Training!

Now let me warn you, developing an EFFECTIVE awareness training program is much easier said than done. An effective program involves all levels of an organization, addresses several time factors, and is . . . ahem, ahem . . . risk-based.

"We require everyone, from the top to the bottom, not just to be aware, but to become involved with the information security process," says Morteza Semnani, SVP Technology and Operations and CIO of First Indiana Bank. And he's right, especially when you carefully read the newly updated Information Security Handbook as published by the Federal Financial Institution Examination Council (FFIEC) in July 2006. It establishes that awareness training should be handled not only at the user level, but also at the management level, and even at the board level.

At the management level, there is a lot that can be done. Involving management in vendor due diligence, operational risk assessments, and data classification makes a good start. But security managers should be teaching policies and procedures, as well as risk management practices. "We have a very structured process, including annual comprehension tests tailored to each job description," says Semnani. "For example, all IT personnel complete annual comprehension tests aligned with the review and updating of mission critical IT policies and procedures. A 97% achievement is required." Semnani's bank uses his intranet for the delivery of the comprehension tests. The grading and tracking of results, which is handled by the compliance department, is also automated.

First Indiana Bank is not the only one using their intranet to facilitate their awareness training program. "We use our portal not only for communicating policies and procedures and training exercises such as comprehension tests," says Gail Koehler, SVP of Technology for Purdue Employee Federal Credit Union, "but it is an essential tool in our Incident Response Plan as well." The portal, developed by Passageways, has become the central communication tool of every employee's desktop. "Thus, during social engineering tests, our auditors end up very frustrated because our people post critical information in real time."

However, an important key is to ensure employees know they are empowered to announce suspicious activity. "The first point of contact posts the suspicion on the portal, then follows the escalation path to report the potential problem to management. That way awareness IS the response."

In other words, awareness becomes a real-time proposition, rather than just an annual compliance task. We encourage our clients to address several time factors: do the annual training, supplemented by monthly reminders and, of course, the real-time incident response broadcast. "It's about due diligence, getting people

INVOLVED in the job of protecting our customers' information," says Larry Turner, CIO of Richmond Mutual Bancorporation. "It's the questions you ask yourself before you act."

And Turner puts his money where his mouth is, having conducted various workshops and seminars not only for his tellers, management team members, and board members, but also his customers. "Actions speak," says Turner. "Our actions tell our customers that their information is valuable and that we protect what is valuable to our customers."

Now I know this is going to seem self serving, but it always does go back to the value of information doesn't it? And the risk to that information, and thus the need for risk assessments, right?

Right?

"It doesn't have to be that fancy. I use the same approach to security I've used since 1967," says Turner, who is not afraid to disagree with me, even in the middle of my workshops. "Back then, you had certain papers you just didn't leave laying around. It was about who had the keys to the locked cabinet. It's the same now."

And I can agree with that, but I still think the risk assessment can be used in developing your information security awareness training program. "The job," says Morteza Semnani, "is trying to decide what NOT to include in awareness training as much as what to present." In Semnani's awareness program, great care is taken in clearing out the noise. "Look at it from a risk perspective. What a particular job description should know is prioritized by the objective of managing risk, and it's not always technology based."

What? Not always technology?

"It's not just the computers," Turner adds, "it never has been. It's about turning the withdrawal ticket around and pointing to the balance instead of blurting it out." And if you look at the stats, information security has very little to do with firewalls and IDS and honeypots, and more to do with the way we handle information. According to a 2006 study by Javelin Research, the majority (30%) of Identity Theft incidents were a stolen wallet. So what we need to do is treat sensitive information the way we would treat our wallet and/or purse. Which amounts to staying on-guard and always being aware!

And Turner agrees, "A big part of the job is to continually ask the bank employee, 'Are you doing your job to protect our customers' information?' You have to stay on your toes."

And Koehler can back up that sentiment from a big picture as well. "Trust is one of our core values. People pleasers are more than willing to help. And that opens us to certain vulnerabilities. If you don't continuously keep your people aware of the threats and vulnerabilities, they'll let down their guard."

Which again brings me back to the risk assessment, because after all, it involves identifying the threats and vulnerabilities? Right?

Right?

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.*