CSO
SECURITY AND RISK
Print Close Window

From: www.csoonline.com

Information Security and the Importance of Context

Those entrusted with information security must raise their contextual awareness, say Ben Rothke and Benjamin Tomhave

Ben Rothke & Benjamin Tomhave, BT Professional Services, CSO

August 29, 2008

When the Transportation Security Administration (TSA) was first created, it created a sudden need for tens of thousands of screeners. Getting a job as an airport screener was a pretty easy process. It seemed as though if you had a pulse, you were in. Jump forward to 2008 and becoming a screener is a bit harder as the TSA has instituted background checks, has upped the educational requirement to include a high school diploma or GED, and added other significant requirements.

There is however, a much easier and quicker way to qualify a TSA screener; one that can qualify a candidate in less than a minute. Simply ask them the following question: What is the difference between Al-Qaeda and the Taliban. If they know the answer, they are hired. If they can't answer it, they clearly lack the contextual knowledge to perform their jobs.

Why is that such a critical question? As a screener, their job should be to keep the terrorists off the planes. If a screener knows the difference between Al-Qaeda and the Taliban, it shows they know the context of one of the many critical threats. If they don't know that crucial difference, all they can do is remove the bottles of liquid that violate the 3 ounce limitation.

Their lack of contextual awareness of the threats creates the mess that airport security is in today, where toddlers are pulled aside and the captain of the airplane is interrogated. What really needs to happen is for the TSA to develop a number of contextual questions, beyond the basic Al-Qaeda/Taliban question. Fortunately, there are thousands of such questions with which to work.

So, how do the issues relating to an absence of context informing TSA screening policies relate to information security? Far too many information security professionals also lack an analogous context: they don't know what true threats are facing their organization. They donâ¬"t know what to look for, where their data is, how to protect that data, and much more. That translates into masses of CIOs and CISOs buying security hardware and software and doing information security things, often in the name of information security, but not knowing why. Things get done in the name of information security, but ultimately, information security is not getting done.

For information security to mature, those entrusted with it must attain the required level of complete contextual awareness. The following 3 steps are required to achieve this contextual awareness:

1. Know your risks. The foundation of any information security program must be a formal and comprehensive risk assessment, whether that be with ISFâ¬"s risk tools (e.g. IRAM or FIRM), RMI's FAIR, or any number of other methodologies. If you don't know your risks, you have no idea of your context, no idea of who your enemies are. You end up doing a lot of security stuff, but do not have much to show for it.

2. Determine protection levels. Once your risk assessment is complete, you need to create a formal plan on how much security you want to deploy. This is a combination of business and technology requirements. You need to find that point where the right amount of security to be deployed is. This determination can leverage any number of prioritization approaches, such as by performing a business impact assessment (see ISF's IRAM, again) or even by leveraging a formal security maturity model, such as SSE-CMM.

3. Create the information security program. This requires management support and a CISO with an effective team and a strong project manager. Many different frameworks can be leveraged in building out the security program, though our favorite is leveraging the ISO 27000 series standards.

Follow those three steps and you will have created a world-class information security organization. But if you blindly buy the security appliance of the month, and chase perceived threats, your security staff will be nothing more than simple screeners. It's all about context. ##

Ben Rothke CISSP, QSA (ben.rothke@bt-ps.com), author of Computer Security: 20 Things Every Employee Should Know (McGraw-Hill Professional Education), and Benjamin Tomhave, MS, CISSP (benjamin.tomhave@bt-ps.com) are Senior Security Consultants with BT Professional Services.