

Anthropology and Awareness.

What Gives?

By Sean Lowther, President and Founder Stealth Awareness Inc.

What does Anthropology have to do with safeguarding sensitive information properly?

“Who cares,” you might say. “I have no idea what Anthropology is,” you retort. Neither did I until a couple of years ago in terms of how it helped understand human behavior in the here and now.

Today, many companies are using Anthropologists to better understand why people do or fail to do the right thing. For example, an employee clearly understands the importance of destroying sensitive information they have designated to destroy. But in fact they leave it in a desk-side receptacle for days, thus easy for anyone to retrieve. In a traditional business environment, there is one behavior. In a remote working site environment, there is often different behavior as it is when someone is working from home.

Never-the-less, in all cases, sensitive information remains exposed under the mental guise that it is somehow safe due to the environment in which it exists. Unfortunately it is not destroyed appropriately or placed in a secure destruction bin and that is the issue. How do you change human behavior to do the right thing?

If an employee fails to destroy sensitive information properly in a timely, effective manner, the penalty could be cutting off the left or right hand. A little severe, but the message becomes loud and clear. O.K., you can't do that, at least in America.

Maybe a voice activated sensor attached to the employee's chair. When the employee gets up, the sensor, which is wirelessly connected to their computer says: “If you are now leaving your desk area, please secure all sensitive information including that to be destroyed and either turn off your computer or activate your screensaver now.”

You can add an additional touch, such as, if the employee fails to do this, their computer will not only time out, but they will have to call 1-800-SUPPORT to have their access and password reset. Or when they return to their work area and sit down, the chair electrocutes them. I know you thought of that.

Though these ideas are far fetched, the problem still exists. We, as American's, have this unfaltering belief that 1) we will never become a victim, 2) the building we work in is secure, thus everything in it is too, and 3) I would never fail the idiots test. The answer to all three is: “FALSE!”

Each day countless employees self-victimize themselves, the companies they work for, and the customers they serve by failing to protect sensitive information properly.

Each day countless buildings are accessed by unauthorized individuals with the intent to steal sensitive information to access systems, commit identity theft or sell what they find to willing buyers.

Each day countless employees prove they are idiots, by failing to follow simple guidelines to safeguard sensitive information properly. That may not be a fair assessment. If you don't train them in the right behaviors and reinforce those behaviors over time, then those unintentional risks just happen. Don't they?

If your organization becomes a victim of an information security incident that can be directly related to a lack of training and oversight, then the failure to safeguard sensitive information properly is not that of the employee. Rather, it's management's failure to understand the risk and failure to not implement an effective information security awareness training program (training, processes for checking, measuring and reinforcing the right behaviors) to ensure the integrity of the sensitive information entrusted to and for the company is adequately secured.

What Sarbanes-Oxley did in response to corporate and accounting scandals, should have similar legislation enacted to step up the awareness of America's business in their responsibilities to safeguarding sensitive information properly when it is placed in their hands. A threat of doing the wrong thing may spur senior management to focus on and do the right thing.

Sean Lowther is President and Founder of Stealth Awareness Inc. He is also co-author of *Techno Security's Guide to SCADA: A Comprehensive Handbook on Protecting The Critical Infrastructure*. He has also spoken at many conferences including CSI and ISSA. You can learn more about Mr. Lowther and Stealth Awareness Inc at his Web site: <http://www.stealthawareness.com>

© 2008 Stealth Awareness Inc., All Rights Reserved