Herding Cats:
Practical Security Tips for a Wacky World

April 2008

BrandenWilliams
SECURE BUSINESS GROWTH

Let us all take a lesson from the Department of Homeland Security ("DHS"), and Ron White.

Wait, what? I doubt that you have ever seen those two entities in a "let's take a lesson from" discussion. What could we possibly learn from them together?

Let's explore the moral of the story first, and then we'll examine how to get there. The moral is "Security designations should include instructions on what they mean to me." If you want to classify data for protection purposes, you should include instructions on what to do with that type of data.

DHS created the National Terror Alert System[1] to convey the current risk and probability of a US terrorist attack. It has five conditions (or colors): Low-Green, Guarded-Blue, Elevated-Yellow, High-Orange, and Red-Severe. If you have the poster from DHS, each condition contains information on what the definition of the condition is, as well as recommended emergency action steps.

Well intended, but it still needs a poster to explain. Unless you have memorized the poster, you cannot look at the condition and instantly know what that means to you, and what you need to do next.

In contrast, Ron White's "heightened state of awareness system" only has two levels. "1) Go find a helmet." And, "2) Put on the damn helmet."[2]

Am I advocating a two level system that goes from "Get Ready" to "It's On?" No, but there is a good lesson to be learned here. Let's take document data classifications. People tend to rely on common nomenclature such as Secret or Confidential. Used separately to label a document, most people could probably figure out that it is a sensitive document. Unfortunately, many companies include them together in their data classification scheme.

If you were presented with a collection of documents, would you know what the difference between Secret and Confidential is? How might you change your responsibility and/or action associated with those documents?

My suggestion is to name your classifications such that the classification term defines what you can or cannot do with it.

For example, "Internal Use Only" always struck me as a self explaining term. Only individuals internal to the company should be privy to this data. The limitation here is simply a timeframe. How long is this data for internal use only? Most internal data will eventually be released to the public. A good example of that is data that is released to Wall Street. Prior to its release it is extremely sensitive, but after its release it is not.

What would an ideal set of classifications look like? Each company should assess their own situation to determine this. But some names that you might consider could include:

- EVP and Above Eyes Only, Release to Public on X
- Internal Use Only, Not for Public Distribution
- Board Use Only until Q1/FY08 Earnings Call

FOOTNOTES

[1] *See http://www.nationalterroralert.com/homeland-security-alert/ for more info.*

[2] *http://www.tatersalad.com/*

The main point is to demonstrate how terms such as “Secret” or “Confidential” do not describe enough about what to do with some data to really expect consistent handling by new, or even experienced employees. When building these data classifications, the following should be considered:

- Who can see the data? Who should not see the data?
- How long should the data be restricted to a certain group?
- Do access levels change as the document ages?
- When can this data be released to partners, shareholders, employees, sales, marketing, etc.?
- When should this data be released to the public or disposed of?

So take a lesson from the Department of Homeland Security and Ron White, and ensure that your data classification system is descriptive enough in the terms such that someone reading the classification understands exactly what should be done with it.

About the Author:

Branden R. Williams, CISSP, CISM, CPISA/M, has been making a name for himself in the Information Technology and Security arena since 1994, as a high school Junior. Now, a graduate of University of Texas, Arlington earning his BBA in 2000 with a concentration in Marketing and the University of Dallas, where he earned an MBA in Supply Chain Management & Market Logistics, in 2004, Williams is sought after as both an Adjunct Professor and Information Technology & Security Strategy Leader in the corporate world.

Williams regularly assists top global retailers, financial institutions, and multinationals with their information security initiatives. Read his blog at or reach him directly at http://www.brandenwilliams.com/.

TEL 214 727 8227
FAX 214 432 6174
BLOG brandenwilliams.com
EMAIL brw@brandenwilliams.com

brandenwilliams
SECURE BUSINESS GROWTH