A Deadly Trend in Cybersecurity

I have been watching with both fascination and horror a new trend in Cybersecurity, the introduction of the phrase "outcome based". Let's dissect this shall we?

The definition of "outcome" per Webster's online:

something that follows as a result or consequence

- a surprising *outcome*
- patient *outcomes* of bypass surgery
- We are still awaiting the final *outcome* of the trial.

Please note, that in the context of the user, it is a result or consequence observed or done to the user. It is not necessarily a deliberate and/or expected result.

So, how are we seeing this used in Cybersecurity? I have seen the entire Security Plan for the Department of Defense (DoD) Joint Enterprise Defense Infrastructure (JEDI) contract state that it is totally based on outcomes. I have seen recent speeches (DoDIIS WW, AFCEA Conferences, etc.) state that "outcome based" approaches are the focus of Cybersecurity today. Why would we want that?

Since we all know there is a shortage in Cybersecurity professionals, and I believe that many of the self-declared Cybersecurity Subject Matter Experts (SMEs) do NOT know true Cybersecurity, we are left with leadership making declarations in order to "help" accelerate Cybersecurity and, most importantly, cover their backsides by making supportive statements. Another possibility, since most organizations can NOT execute Cybersecurity correctly and most people can NOT provide detailed examples of how to improve (or worse, leadership makes the conscious decision to not invest in what they are being told), then the leadership has created this great sounding construct of "outcome based" approaches. What they are really saying with this statement is:

"Since we can't figure out how to make really good sausage, let's just focus on the packaging and how we provide sausage to the market. The outcome is what is important, the how doesn't matter."

I hate to be the bearer of bad tidings, but that standard will NOT support the evidentiary based approaches required of today's Cybersecurity. Not only do you need the proper Cybersecurity Awareness, you have to build into every decision Cybersecurity Resiliency. And for you Federal Government (and contractor) types, you have to ensure your evidence shows you did NOT wittingly, unwittingly, knowingly, or unknowingly compromise National Security. That can't be done with "just get-r-dun" attitude. Just like DevOps is a short cut to development that has many risks inherent in its approach, so too, is "outcome-based" Cybersecurity.

A Deadly Trend in Cybersecurity

When will people, employees, leaders, organizations and our country realize, good Cybersecurity is like Citizenship? YOU HAVE TO WORK FOR IT!

For Additional Information Contact:

Eigenspace
312 Main Street, Suite 300
Gaithersburg, MD 20878
240-654-4097
www.eigenspace.us