Cybersecurity Spend and Why?

I'm fascinated by the news (not the fake news debate) about the projections by analyst firms about Cybersecurity spending. See this article as an example: https://www.helpnetsecurity.com/2018/03/30/spending-security-solutions-2018/

If we are spending more and more individually, corporately and as a country, then why are the breaches exponentially increasing? There has been an explosion of the number of companies who are "Cyber companies" and here to help. Yet we see no end in sight to Cybersecurity spending and no relief from the attacks (both successful and not). How did we get here? Is there a better approach? Can we stem the tide of insanity?

Further observations, I believe we can group all commercial Cybersecurity organizations into three groups: a) Niche Cybersecurity products, b) Consultancies (mostly aligned behind their progenitor who has some Defense or Intelligence background), or c) Large Integrator/Contractors who politically can't be a serious player in the market without a "Cybersecurity" organization somewhere within.

Let's break this down further. Cybersecurity Niche product companies sell you a product (or more) that addresses a particular Cybersecurity problem you have (either a known problem or not). This has created multiple products to solve the same problem(s). Multiple products may also overlap in other areas of the Cybersecurity problem. It is up to the buying organization to understand the Cybersecurity spectrum and what product covers what part of the Cybersecurity spectrum. When an organization is struggling to understand the entire Cybersecurity spectrum, then how can it know where these products fit and where they don't, yet it is their unadvertised responsibility to figure this out?

Next, the consultancies. Since most of these types of companies are a based on the legacy of their proprietor, how is the thousand employees of these companies just as experienced, known, published or capable? They really aren't. And, as one of many customers of these organizations, are you really getting that famous person's undivided attention? What do you really get on contracts like these? Contractors who have a certificate or certification but little practical knowledge (there are so few who are superstars, right?). This creates a very difficult situation. Please provide some personnel who are "Cybersecurity experts" and they are few and far between, but we, as contractors, have an obligation to try to deliver anyway. These contractors sell hours of work to organizations based on their leader's lineage, they may or may not have the experience, education, knowledge, experience, skills, or abilities required to be fully successful over the broad expanse known as Cybersecurity.

My favorite area is the medium to large company that has created a Cybersecurity Division to be relevant. This Cybersecurity group has very little say over the establishment. This group will

Cybersecurity Spend and Why?

struggle with staffing, training, providing insight and research, and, most importantly, delivering to the customers consistently successfully.

What I believe is the fundamental issue from all these observations is all offerings from these three type of Cybersecurity companies are targeting the struggling customer who has all the burden to understand the Cybersecurity Landscape and how each of these types of companies engage to solve what portion of that Cybersecurity Spectrum. How can these struggling companies compare "apples" to "apples"? We need a common vernacular and assessment model for all companies and align their offerings and products to this standard. We can then begin to communicate in the industry differently. Something like, "Mr. Customer, we have the best in the market to solve 'C, D, E and F' from the A through Z Cybersecurity continuum. We are better at solving these issues than our competitors for the same E and F categories." Then the conversation can focus on the piece that is really missing in the assessment side, what Cybersecurity Controls are these offerings, processes, or products actually mitigating for me? While I now have a standardized Cybersecurity Landscape to communicate with customers and partners, what does each part of my portfolio of offerings or products solve for you Mr. Customer?

This honest discussion with common vernacular and a real discussion of impact to the Cybersecurity Continuum is where we must mature to make this better for all. It is our own fault (the Cybersecurity Industry) that we are in this conundrum. We are in a Cybersecurity fight in an extremely complex and heterogenous technical environment that we don't understand. These organizations are asking for help and we are all trying to reply on our own, in our own ways for our own ends. Organizations are struggling to make "heads or tails" of these Cybersecurity challenges. They can't do it themselves. BUT, the cure is just as bad as the disease in this case. We can and MUST change the conversation so that we can begin to help organizations have a clear picture of their responsibilities, challenges, and focus on the right things by not expending energy on navigating the mess we have created in supporting these struggling organizations. I call on the Cybersecurity Industry to step up for the good of ourselves, our customers and our country.

For Additional Information Contact:

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