All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Three Little Words

Hint: They are not "I Love You" (although those are the 3 little words in other contexts).

I sometimes become tainted by dealing with too many folks who are just getting started in cyber security, and forget that there are a whole lot of folks who are really doing a great job. I was reminded of this at the Tech Vision Research Chrysalis conference last month.

One of my favorite experts from this venue is Doug Simmons. He did not disappoint, particularly a week earlier when I was working with him on consulting gig. He put into 3 words what often takes me a paragraph (and in this case a whole page):

Crawl Walk Run

We commonly develop 1, 3, and 5 year plans for enterprise protection programs, and this is usually a reasonable amount of time to develop and start to mature a program. And yet, all such programs start somewhere and get to somewhere else over time.

- **Crawl**: They start slow and only get so far in a short time.
- **Walk**: They start being able to go where they need to go, but at a limited pace.
- **Run**: They get to where they can handle anything that comes up in a timely manner.

People in the cyber-security field often find it hard to recognize the reality of organizational operations. They are often in a rush to do what they consider to be direct and straight forward things. They tend to argue technical points and not take into account the politics of the situation. And they imagine that what is obvious to them should be obvious to everyone else.

A quote from Virgil Gligor comes in handy here:

"If you think about it intensely for three years, it's obvious"

It takes time to build a cyber-security program. It has to be properly fitted to the entity it operates in. Some mistakes will happen along the way, and we have to be careful that the consequences of those mistakes are limited. Such programs need to become mature within their context, and that means doing everything a first time, then repeatings it, documenting it, measuring it, and ultimately managing it as a systematic part of operations.

It's not the hero's journey

When I tell people I work in cyber-security, they think (and say) things like "that must be very exciting". But the heroic actions of individuals saving the day is not the goal of a successful cyber-security program. That is what happens when the program is not working well. We should not be smiting dragons. We should be working on running a successful program that becomes normalized over time and continues to adapt, with limited and predictable outcomes.

Conclusions

A successful cyber-security program should appear to be mundane, methodical, and have few or no surprises. Crawl, walk, run, and systematically develop a mature program over time.