All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

It's a race, and I just said "Go!"

It's 15 years now that Cyber Security Awareness Month has been running, and I thought I might update you on what I did over and around the last month to help improve the situation. Hopefully you will take advantage of some of these things and work toward improved cyber security awareness yourself over the remaining 11 month-long opportunities of the year.

It's been busy

For some reason, there seems no end to the things you can do in this arena. One of the things I did recently was a trip to India to help faculty in a University become more aware of the issues. In the US, there is a widely published need for something like 1 million more experts than we have today. India has something like 4 times the population, so simple extraction says India needs 4 million. China needs perhaps 6 million. That's a lot of millions considering, for example, that there are only about 120,000 CISSPs in the world. That's up by about 10,000 from 2 years ago.

My estimate was that, if you need 4 million people with expertise, you should be educating and training something like 400,000 every year for the indefinite future. That's because careers only last so long and people move on to other things along the way. At 400,000 per year, it would take 10 years to fill India's needs for today, assuming every one of them was still working in the field in 10 years. Of course if you want to meet the need sooner, it will take more effort. But whenever you have it in place, careers typically run about 30-40 years, and at least half the folks in any one area will move into another area over the course of their career. So sustaining 4 million experts would take an ongoing effort to keep producing between 100,000 and 200,000 per year after spending the first 20 years producing 400,000 per year to get caught up. I'm getting older (as are we all), and don't want to wait that long.

How many can you train/educate?

The largest educational program in a related area I helped to develop (with Tom Johnson) was the one at Webster University, which as of last year was producing something like 600 graduates per year with MS degrees. But that's a drop in the bucket compared to 400,000. How do we scale this by a factor of 1,000? Every CISSP on the planet could take on 4 folks as apprentices. That might be able to get it for India if they could learn all they need to know in one year as an assistant. But then there are the other 5 times as many jobs required for the rest of the world. 20 apprentices per CISSP is a bit much. Here's what we came up with.

We are starting to teach in October using online education. It's an imperfect, but scalable approach. We hope to have the first 500-1,000 students taking the first course in November, and we are coming out with a new course every month for 12 courses over the period of a year. The goal is to produce graduates who can do an actual job, at entry level, in cyber security, in every class. So if all you want to do is learn how to detect attacks on networks, you should be able to learn and practice enough in one month to start working in 4 weeks. If you sign up November 1 and pass the course, you could have the entry level skills to get a decent job December 1. The Vice Chancellor already committed to 500 scholarships...

Over the next year we hope to offer each course as we grow them, every month. So by the end of the year, we hope we will have produced something like 6,000 people (on average) able to work in each of 12 different fields, enough to take 72,000 jobs, if each student only took one course before starting to work somewhere.

If we get proper support and the methodology works, we might even be able to get to that point for 400,000 students in 2019, and be on track to build the necessary capacity for India over the next 20 years. But of course that's not enough. So if we get this going at scale in India, we will start offering it worldwide after that. It includes laboratory exercises, lectures, homework, tests, and the ability to answer questions from students.

Here's the deal. I want other educators to try to compete with me. It's a race, and I just said "Go!" How many students can you educate to the point of getting a real cyber security job by the end of cyber security awareness month in 2019? I want to hear from you, so get going!

New talent is not enough!

Another aspect of the cyber security awareness challenge is getting executives to understand the nature of the issues so they can start to address them in a reasonable way. Making CEOs aware is a necessary condition. But how do we do that? Here's what I did in October. Using LinkedIn, I connected with CEOs from entities with more than 500 employees. Not just a few of them. I think by this writing, it's well over over 1,000.

I provided them with articles I hoped they would be interested in. One on duty to protect (474 views), one on standards of practice (1073 views), the ONE page your board should read (501 views), one on trust (513 views), and just recently, one about the Cyber Security Brain (670 views). I interacted in non-trivial one-on-one messages with scores of them. Many of them asked me why I wanted them to read the articles, and I told them that I was interested in their opinions and questions, which is true.

So that's something like 1,000 CEOs who are actually more aware today than they were a few months ago regarding cyber security issues. We also communicated with CISOs, and some of them indicated that they shared them with others in their enterprises.

Here's the deal. I want other consultants and experts to try to compete with me. It's a race, and I just said "Go!" How many CEOs can you get to read an interesting article you write to the point of having an actual exchange of thoughts about it with them by the end of cyber security awareness month in 2019? I want to hear from you, so get going!

Better business approaches

As many of you know by now, I am also an angel investor and work to help startups succeed. One of the things we do in this space is called due diligence. Due diligence is supposed to be an independent objective review, in this case, of an investment opportunity, by a potential investor. I am the lead for the "secure cyber" group at Keiretsu Forum, the most active private angel investment group in the world. As such, I see a number of early stage companies that have potentially serious negative consequences to the investors associated with cyber-related incidents.

As part of this effort, I often get questions from other investors, DD team members, startups, and others about cyber security issues. They range from personal incidents of being hacked to questions about trillion dollar markets being disrupted by new technology.

None of us know everything about cyber security. So I attend lectures, discussions, and panels of experts to stay up to date by learning from others. It happens by pure chance that in October I started a due diligence efforts for a business that could become a major player in a multi-trillion dollar market, and where that company is making claims related to block chain technology. It also happens that earlier in the month I was at the Electronic Crimes Task Force meeting where the panel was discussing block-chain and crypto-currency transactions, tracking, frauds, and related issues. It also happens that I wrote one of my 50-ways articles in the last few months in the area of how to defeat your block-chain and crypto-currency system.

I haven't formed any opinions regarding that particular business yet, and likely won't for at least a month or two, depending on how much information I get from them how soon and what it indicates. But I have formed a more general opinion about the – something like 100 claims I have heard from other block-chain companies in the last few months.

My opinion is – it's about the business, not about the technology.

This is not a new concept nor is it original to me. Whenever I hear about an AI, deep learning, cloud-based, block-chain, whatever, it triggers in my mind the meme:

A breakthrough in marketing technology

That's a phrase we came up with at Burton Group (although someone else probably had it before us somewhere else) when I was an analyst in their Security and Risk Management Strategies group. It means that they have found a better way to scam …. oh… ah... sell.

Here's the deal. I want other analysts to try to compete with me. It's a race, and I just said "Go!" How many companies in the cyber security space can you help to stop selling BS and start talking about the real business value they bring? And how many investors can you get to understand that the claims do not match the realities of what the technologies do by the end of cyber security awareness month in 2019? I want to hear from you, so get going!

Conclusions

Here's the deal.

I want all of us to try to compete with each other over how many decision-makers we help to better understand the issues in cyber security.

It's a race, but a friendly one. And I just said "Go!"

Winn Schwartau gave away and sold hundreds of thousands – perhaps millions of his early book on cyber security for children (and their parents).

> Can you write a more popular one?
>
> I bet Winn will be happy to help you publish it!

I am going to try to teach more than 100,000 people enough to be useful in new cyber security jobs in the next year.

> Can you teach more?
>
> I will be happy to help get your course in front of as many folks as I can.

It's a race. And I just said "Go!". I hope we all win, but I'm planning to do my best to beat you. In a friendly sort of way.

