All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Not Pearl Harbor – the boiling frog

As I was thinking about this month's year-end article, I was seeking an analogy that wouldn't get into the political arena or the fear mongering. There is increasing clarity and recognition that cyber-security is in a sorry state and increasingly important to all aspects of human life. It effects us all, directly or indirectly, and everything from elections to revolutions to ecological disasters to personal losses follows from it. The best thing I have come up with so far is an ice age, even if it is on the wrong overall time frame.

Not with a boom, but a whimper

The vast majority of the cyber-technology establishment worldwide has not yet come to realize what is involved in securing systems against intentional malicious threat actors. Those who don't get it, or get it but don't know what to do about it, tend to fantasize about the single event that causes the end of their world as they know it. Everything goes down – it's all over. Of course that can happen, but that's not likely how it will go. Rather, instead of a big boom – the cyber Pearly Harbor – whatever you may fear – it is more likely that our freedom and our free flow of information world will end with a slowly tightening noose of controls. These controls will be imposed by governments because the people will call out for them, and those imposing them will tell us that if you're not a criminal you don't have to worry. Then they will make it criminal to do almost anything and it will be too late to worry. We march willingly to our own demise as the age of reason turns to the age of disinformation, deception, and demise.

Not with a miracle cure

Or not! The biggest problem I see today, among both the ill-served clients and the cyber security elite, is the miracle cure approach to saving us after each local disaster. The normal process today and for many years has been this:

- Normal state of entity – roll along like nothing bad will happen – ignorance is bliss.
- Bad thing happens – top management gets scared – must act or at least appear to.
- Top management acts – demands miracles from staff who are normal humans.
- Staff sees opportunity to do what they wanted to do and asked to do for years.
    - Alternatively – staff afraid of being fired – calls in outside expert
- Urgent mitigation happens – costs gobs of money – also identified 50 other problems.
- Entity working again (or failed) – normal state declared – nothing changes – bliss.

The miracle cure approach happens each time you get a heart attack – until you die.

That is how we got to where we are today. The vast majority of entities operate in the miracle cure world. They buy into the religious view of cybersecurity and the healers who come at a very high price when you need a miracle waive their hands and do their things and you are cured. You may be free of the pain in your side associated with the stick that pierced your skin, but you likely still have the infection that caused you to slip and fall on that stick.

But with a healthy lifestyle

I know analogies are imperfect, and the whole infection, stick, falling thing are not even really deserving of your toleration. However, you likely bought into that if you bought into the whole miracle cure thing, so why should I work to find a better analogy when you will buy into the first snake oil salesperson who tells you UTM-venom cures cyborg-pneumonia?

The way out is for the world to change from the miracle cure version of cyber-security to the preventive medicine approach to keeping health care costs down. Not that we have really embraced this in the health care arena, but that's another story altogether.

The way to freedom and prosperity in the new year and the new age is through a systematic comprehensive – (shall I say boring, thoughtful, workman-like?) – approach to learning how to do the cyber-security job well and then doing it well. Try this approach:

- Every day and in every way – we do a reasonable and prudent job of cyber security.
- Bad thing happens – we knew something like this would happen and prepared for it.
- Management at the right level responds as planned – there are mild surprises.
- The fixes work reasonably well and quickly – everything's fine again.
- After-action figures out whether and how to do it better next time (part of the first step).

How do I live right?

Ah – there lies the rub. People who spend their time studying these issues and work to stay up to date in all of the aspects of protection are what we need. Leaders who are hard working, well-read professionals with years of management experience and technical understanding, supported by professional staff who work to be good at what they do, stay informed, and operate in a mature manner, working in an environment which rewards professionalism and provides the time and space required to do tough jobs well. They need the right amount of power, influence, independence, resources, etc.

Of course in the lean mean reality of today's business world, there are few such positions, and they are reserved for the most important members of the critical teams for businesses. So act like your life and business depends on it and build/buy these people because – guess what? Your life and business do depend on this. As I said in the second sentence of this article "There is increasing clarity and recognition that cyber-security is in a sorry state and increasingly important to all aspects of human life." So maybe if you start to recognize this you will start to understand that this is a priority of critical strategic import.

Conclusion

Like I said in the beginning of this article, we are the boiling frogs. The temperature slowly goes up, and the frogs cannot tell they are boiling to death because they keep adjusting. If you dump them in the boiling water without the slow warming process, they will jump out. So now that you know the water is coming to a boil, will you decide to boil with it, or will you jump out?

If you read this and say "if only my boss would understand this" - or "if only the CEO would understand this" - perhaps you should send them a copy. Anonymously if you are afraid of getting fired. Jumping out is a lot different from getting thrown out...

