All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

There is no “best practice” or “100%” in Cyber Security

I have seen many companies claim to follow “best practices” or have 100% secure somethings. Rest assured, **there is no such thing**. Hyperbole and selling fear and easy resolution are the hallmarks of poor quality companies in this space. Either:

- **They don’t know - OR**
- **They know and are misleading**

I am not certain which is worse…

Reasonable and prudent:

There is a notion in the law of “reasonable and prudent”, which is to say “diligent”. While the formal definitions are a bit more complex than this[1][2], it goes something like this:

- **Reasonable:=** rational and appropriate
- **Prudent:=** it doesn’t ignore what anyone who looks carefully can see

Putting it the other way, here are some examples of what is NOT reasonable and prudent.

- **Unreasonable:**
  - We spend $10M to protect $1M.
    - We decide to put protection in place because the vendor claimed 100% security or “best practice”.
  - **Imprudent:**
  - We expose our most valuable assets to unnecessary hazards.
    - We leave rocks outside of glass windows with something worth stealing in plain sight behind the windows.

Selling FUD

Many in the cyber security arena sell based on fear and resolution. The idea is to make you afraid and then tell you it’s all OK if you pay them. That’s commonly called Fear, Uncertainty, and Doubt (FUD).

[1] Nolo’s Plain English Law Dictionary says: “Just, rational, appropriate, ordinary, or usual in the circumstances. It may refer to care, cause, compensation, doubt (in a criminal trial), and a host of other actions or activities. In the law of negligence, for example, the reasonable person standard is the standard of care that a reasonably prudent person would observe under a given set of circumstances. An individual who subscribes to such standards can avoid liability for negligence.”

[2] Per The Law Dictionary (https://thelawdictionary.org/due-diligence/): “What is DUE DILIGENCE? Such a measure of prudence, activity, or assiduity, as is properly to be expected from, and ordinarily exercised by, a reasonable and prudent man under the particular circumstances; not measured by any absolute standard, but depending on the relative facts of the special case. Perry v. Cedar Falls, 87 Iowa, 315, 54 N. W. 225; Dillman v. Nadelhoffer, 1G0111. 121, 43 N. E. 378; Hendricks v. W. U. Tel. Co., 120 N. C. 304, 35 S. E. 543, 78Am. St. Rep. 058; Highland Ditch Co. v. Mumford. 5 Colo. 330.”

FUD is a Bad Fad

FUD doesn’t (don’t?) really get you anything as someone trying to be reasonable and prudent (duly diligent) with regards to security. If they make you hyper-vigilant, that can be good, for a while. But if you live in fear, you will not move forward or advance the world.

In essence, in order to be duly diligent you need to know and do your duty. So if you take the time and effort to identify your duty to protect, you can perform that duty in a reasonable and prudent manner. No duty I am aware of includes being afraid. Uncertainty is the nature of the world, and doubt is often a good thing. But the key is to understand your uncertainty as the envelope of futures you face (the risks) and doubt as the reasonable questioning of claims made.

It’s fundamental… **We take risks for rewards.** The question is what risks for what rewards?

Too good to be true

Taking the “too good to be true” option is, essentially always, a bad bet. And that’s what you do when you fail to question or decide to believe anything like 100% in cyber-security.

- Just for clarity, **the numbers count**. I have seen many folks assert that a cost approaches zero as the volume increases, but of course it never reaches zero, which is to say, if you lose $100/ea at volume 1M **($100M)**, and reduce that by half at 10 times the volume **($500M)**, that means you lose 5 times as much. There may never be a level at which you break even, and even if there is, you may never reach it.

And a real example from cyber security:

- A really good spam email detector might detect 99.999% of all spam emails, and let’s imagine it has 0 false positives (which it never does).
- That means that out of the perhaps 10M emails hitting a medium sized enterprise a day, only about 100 will get through. So that’s 36,500 successful spam emails a year.
- If your people are really well trained and know what they are doing, perhaps only 1% of these emails will end up in a person mistakenly clicking on a button. That leaves only 360 successful attacks gaining insider access to your systems and networks per year, or one every day.
- If it takes you on the average 10 days to detect and get rid of each of these, you will, on average, always have 10 successful penetrations operating on your network.

There is a very big difference between 99.999% and 100% in cyber-security. And 10M attempts per day for a medium sized enterprise is not unusual.

Perfection is not attainable – so stop trying

I have been told that I am a perfectionist. Which is another way of saying I am imperfect and know it. I know I make mistakes and I know that each mistake can cause bad things to happen. For many years I feared ever making a mistake, and along the way, I made many mistakes, mostly as a result of that fear. While I still try not to make mistakes, I also understand that if you never make a mistake it likely means you never did anything useful. I decided instead to back off of perfectionism and move toward reasonableness. I spend enough time to try not to do too many stupid things and try harder to not do really stupid ones.

Ending the hype

I started working professionally in cybersecurity in the 1970s. When I became the “principal analyst for security and risk management strategies” for Burton Group in 2001, I was amazed at the extent to which companies suddenly got serious about addressing my questions. Prior to that, I would ask, they would deflect, and there was nothing I could do about it. But as an industry analyst publishing papers read by decision-makers and decision supporters in many large enterprises, the companies I asked had to answer and find a better response. Power is a strange thing in that way. So I decided to use this new-found power to try to end much of the hyperbole around cyber-security. I do that by pointing out the obvious, or at least the apparently obvious once I point it out.

I was intolerant of hype in the 1970s, as I am now.

> *At a conference long ago, a vendor claimed that they had **a system** that “**could not be broken**”. They used those actual words. Their demonstration system was on a table at the edge of a 2-story high drop to a marble floor in the conference center. I asked how much they wanted to bet. They said some ridiculously low number, a few tens of thousands of dollars or less. I said, ~“so that’s the largest value we should trust it to protect”. They were unhappy with that, so I told them I would demonstrate I could break it for free right here if they would stop making this claim. They said sure. So I picked up the system and held it over the railing to drop it. They gave up.*

Here’s the point. Even if they were talking about something else, making clear statements is important in claims about ‘security’, as well as other things we may come to rely on. And you can rest assured that even taken in the context of their claim of “unbreakable”, which they did not make clear, I am certain that their system could be “broken”, for any meaningful definition of that term.

> **The fact they they would only trust it enough to bet a few tens of thousands of dollars on it is a clear indication to me of the threshold of trust we should place on it.**

Consider this.

> **The average ‘bug bounty’ for finding a worst case complete takeover of control ‘exploit’ in a commercial systems today is (per multiple sources) less than $10,000.**

If we judge security by the amount the folks providing it are willing to bet that it works, we will find that security at the level desired almost certainly cannot be purchased for any substantial entity. Security is something you do, not something you buy. Part of the issue here is that your use of their systems has more to do with whether your security fails than the inherent nature of their systems. That’s because reasonable and prudent are contextual concepts.

Conclusions

There is no “best practice” in cyber security. There are reasonable and prudent practices. And what is reasonable and prudent is not a fixed generic answer. It is highly contextual and depends on a diligent effort to find and do your duty to protect.

There is no 100% perfection in anything, and security is no exception. Rounding to 100% when it’s really only 99.999% (or 99.9999%) still leaves plenty of bad things happening.