# All.Net Analyst Report and Newsletter

***Welcome to our Analyst Report and Newsletter***

### The do nothing defense

Of course until you are successfully attacked, doing nothing about security is a great approach. It saves money and time and costs you nothing. So lots of folks do nothing, or almost nothing, and I include myself in this latter approach – almost nothing.

### As little as I can get away with

I do as little as I think I reasonably and prudently can to defend against notional threats that may decide to get at my systems and companies. On the other hand…

### But no less

So what is the minimum I can get away with? It's all driven by consequences, and I have decided to minimize or diversify these wherever feasible. It's a matter of risk avoidance and disaggregation.

### What do I avoid?

Here are some examples:

- I try to synonymize at data entry. That is, instead of naming a client, I use a number, like 32874, chosen not quite at random. Then I use first names instead of full names, and I replace location names and addresses by X-SITE or similar things, where X is a known internal name for the site, or the state in which it resides, etc.
  - *Yes – I know – bad folks can possibly put it all together to figure out who it is, but on the other hand, it makes it harder for the bad folks and no harder for me.*
- I don't collect credit card information – I let the credit card processor do it. In this sense I have transferred the cost and complexity to them.
  - *OK – so this is risk transfer – a form of avoidance from my perspective.*
- I don't load software not needed into systems serving the outside world.
  - *So if they break in, it has to be through a known path that I need to have in place to serve the customer, not some unnecessary path just left there because… why?*

### What do I do to disaggregate?

This is more like an investment strategy. I diversify my efforts, content, capabilities, computers, and resources so that if anything fails, I don't lose everything. Of course from a personal perspective there are things that are precious to me and unique. Examples include my life, my wife, my kids, their families, and so forth. We know they will eventually be no longer as will I, but we do our best within reason to keep them all safe.

When I was younger, I had the notion that when you have nothing, you have nothing to lose. So you can take bigger chances seeking more uncertainty because the downside is less far down than the upside is up. But the more you have, the more you have to lose, and of course you should reasonably become risk (that is uncertainty) averse as you have more to lose.

  

### So it comes down to consequences

Consequences of different futures drive the defense against undesired futures and the offense toward desired futures. And the consequences are different for different sorts of things that can go good or bad.

### Enough of the CIA

I cannot believe that the field of cybersecurity continues with the meme of CIA. Confidentiality, Integrity, Availability, in that order. This is foolishness as a generality, but of course in some specific cases it may be prioritized that way. But let's start by expanding the field:

- **Use control:** Who or what can do what with who or what?
- **Accountability:** How do we attribute actions to actors?
- **Transparency:** What should be externally verifiable and to/for whom?
- **Custody:** How do we know it came from where we think it came from?
- **Reliability:** How do we know it reflects the reality we think it reflects?
- **Authenticity:** How do we know it is what it claims to be?

### Functionality

At an even deeper level, there is the fundamental, that the utility of the systems we create and operate is that they produce the value they are intended to produce. Because ultimately, the purpose of systems is the functions they perform, even if those functions are the perception that they perform some functions that they do not actually perform. All of these other attributes have to do with aspects of utility related to their ultimate functionality.

So I generally start by thinking about (and writing down) the reasons I have systems, content, mechanisms, etc.; what they do for me (where for me includes for people that pay me to have them there for them); the consequences of them failing in terms of the various issues listed (almost always confidentiality is not a priority for me, but reliability and authenticity are very high on my list), and then I think about whether it's really worth doing some of the things I could do instead of other things that might be better but are a lot harder.

### It's about my choices

I happen to have spent a lot of time in this world and I know of a lot of different ways to do the things I want to do. Experience helps a lot. So I have more choices I can make than a lot of folks who don't know what the choices are and decide not to pay experienced folks to help them identify alternatives or spend the time and effort to learn about alternatives.

I make lots of these alternatives freely available on my Web site and let folks know about them on a regular basis. Most folks just ignore these things I do for free, or don't want to spend the time to learn it when that can get it for more money in less time. It's my choice to try to help as many people as I can, and for free is fine if I write it once however I like.

So as a result of this free strategy, I simply put things on my Web site without controls over confidentiality. As a result, nobody really tries to break into it except by the normal random crap they throw at it. Since it doesn't do anything fancy, it doesn't have all those vulnerabilities associated with handling your money, and so it's more secure, I do less, and help more.

  

## Doing nothing

When I say I do nothing, it's not quite true. Most of what I do for securing my own systems I did many years ago. As long as nothing changes, nothing is likely to go wrong. Except of course, the world keeps changing, and in many cases, in doing so, creates problems for me.

Earlier today, Google started rejecting my emails to my own lists. They called my once a week email to the lists spam, but after a few hours on the phone they finally figured out that they might have something wrong in their setups. I had followed their various online advice, changing settings repeatedly, and so forth, and finally, they told me to do something that caused my Web sites to become unavailable for a few hours. While I undid it once I became aware of the outage, they gave me about 5 different bad pieces of advice in their efforts to help me fix what they broke, and it broke more things.

In essence, the problems I have, failures of availability mostly, stem from stupid "security" changes made by providers who are ignorant of the realities of most users who just want to get the job done and not be pestered by their eternal desire to make changes. They trust people who are not reliable and don't trust people who are. That's because they are now trained to distrust people, and of course the zero trust meme has made all of our days more painful by adding multiple authentications to everything, including the authentications themselves. Security load explode! Read the free article and watch the video at all.net ...

## Do as little as possible

Not all solutions are big company solutions. Small companies, that is most companies, can get away with doing nothing but:

- Picking the right outsourced providers and suppliers
- Doing initial configuration management
- Using backups and recovery wisely
- Having some well thought out and reliably executed procedures.

These can be done without IT staff, by following a **good template** that is **semi-customized** to the business type and then **customized** to the individual company.

## How to get a good template properly customized to your needs?

This is where a sensible advisory service comes in handy. Good advice that can cost only a few thousand dollars a quarter can help you do almost nothing else and be reasonably safe. Of course the problem is where you would get such advice. Of course we offer such a thing through one of our little companies, and I should try to sell it to you here, but I won't. Because it's my choice to help you for free as much as I can, and they will sell it just fine.

## Conclusions

The **do nothing** defense is sensible until things go wrong. Doing **almost nothing** until bad things happen is actually a good idea in many cases, and a pretty good defense for most small companies. The devil, as they say, is in the details.

So watch this space and get your monthly dose of **almost** free (you pay for the Internet access and devices and I pay for mine too) advice, and get in touch when you want to do **almost nothing**. I will help you for a little something.

  