# All.Net Analyst Report and Newsletter

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

**Keeping your cyber security program exciting!**

The Capability Maturity Model notions that, starting from scratch, a program matures by going through phases.

- **None**: What is being considered has never been done (here) before
- **Initial**: Heroic efforts by individuals makes something happen the first (few) time(s)
- **Repeatable**: The same thing can be done again with the same results
- **Documented**: The activities are documented as planned and executed
- **Managed**: Someone makes sure that what is supposed to happen does/did happen
- **Optimizing**: It is adapted over time to improve performance

I have noticed over many years that most cybersecurity programs I encounter are barely operating at the repeatable level.

**Cyber Security as Sexy!**

Many hero types like the heroic effort thing. They feel proud of their daily heroism and accomplishments in emergent situations. I tell people I work in cyber security and folks say things like “Wow… that must be exciting / interesting ... you must be very busy!”

But for the enterprises we work for, this situation is usually an enormous problem.

**Cybersecurity properly done is not a thrill ride**

**It should be mundane, every day, and systematic**

**Expected events with expected outcomes**

Unfortunately, this is largely not the case. The reason for this is that most programs are not matured, and this appears to be because most companies are not seeking to mature them in a serious way.

**Why don’t they invest the necessary resources?**

Most executives I meet would like to run well-managed organizations, but many of them lack the basic skills and understandings of how to do this. As a concept it is relatively easy to do, if you have adequate resources in place. Of course most companies are trying to minimize resources for things like cyber security, reasonably because it is viewed as (and often is) a cost instead of as an enabler.

Consider that spending another dollar on sales (depending on the company) brings in another ten dollars in revenue and three dollars of gross profit. Spending another dollar on cyber security spends one of those three dollars of gross profit, leaving only two.

Getting to managed maturity, if it is expensive, will be delayed, and increased sales will be preferred. But it doesn’t have to be expensive. In fact, it should make things less expensive if well and properly done.

  

**Getting to Managed is not that hard**

If you think for a minute, it's pretty easy to get to repeatable and documented. Here's how:

- Whatever you do, take notes – or record it – or keep good audit trails – or whatever
  - Congratulations, you have now documented what you do.
- After you do it the first time, create a checklist
  - Congratulations, you now have a **documented procedure** to follow
- Next time, follow the checklist and update it for changes/improvements/alternatives
  - Congratulations, you now have a **documented repeatable process**
  - Don't forget to keep copies of all of this for an appropriate period of time.

Note the lack of required technology. You can do it, and for centuries this has been done, with paper and ink. However, in the modern age, we can use a computer do do this.

- When something happens, the documented repeatable process should be used.
  - That's definition of the process is called the **Plan** (ISO 2700), and when you use that process, you have undertaken the **Do** part (ISO 2700).
- A manager in charge of the process should review the checklists against the outcomes periodically (at least once a … depending on the consequences of missing things).
  - This review is called the **Check** part (ISO 2700)
- The manager, in the review process, should be looking for failures in the process. When this happens, they should fix the failure. That's the **Act** part (ISO 2700)
- Congratulations, you now have a **managed** program.

Here's the really tricky part (for advanced readers only). If you improve the checklist based on what you learned from the failures, you are **Optimizing**.

Now do this for all of your cyber security activities, and you have a managed (or perhaps even optimizing) maturity level over all. That will, of course, include the processes of doing new things. If you copy the last few sections of this document, **you now have a documented repeatable procedure** to follow **for getting and keeping your program managed**.

All you have to do is Plan, Do, Check, and Act on this documented procedure and you will have a managed program!

**But I don't want to!**

Is sounds so easy when I say it. But actually doing it is really where the problem lies.

- People tend not to document what they do well – or contemporaneously
- People don't usually want to go back and try to write down what they did and test it to see that it works so they can do it again and again.
- People really don't like having to do this for lots and lots of things… boring!
- To be clear, this is not my favorite thing, and I sometimes stop doing it – for a time.

  

### But that's what computers are for!

Yes indeed, computers can make all of this easier! And people have all sorts of systems to help do this. For the more sophisticated among us, this means a workflow system!!

- Now we have overhead! We are really getting sophisticated

However, a workflow system takes a lot of time and effort to get going, and more time and effort to keep going. Instead of a piece of paper with a list of things to do that we can copy to do them again and repeat the process and document it and review it, etc. we now have a client server architecture with programmers constantly reprogramming the new sequences of activities and approvals, and we produce complex metrics analysis outputs in graphical form for management reporting that proves we are efficiently doing – what might be the wrong things… because when we over-automate, we may also under-think.

The cool thing about the hero culture is that it keeps people interested and paying attention.

### It takes time to mature

I could be talking about people here, but I am talking about a cyber security program. And there are lots of simpler systems that allow you to do parts of this process without the big integrated unified workflow engine. I personally develop tools to support my various businesses and these allow startups to very quickly reach documented and even manged. And even though they are not all that sophisticated, they do allow management to do its job at some reasonable scale until they are ready to take on the much more complicated job of running enterprise systems to manage their business.

But even in my relatively simple systems, it seems to take a lot of time to get people to use these sorts of mechanisms and systems, and we almost always have process faults along the way, if only because people just cannot stand to keep plugging away as if they were machines day after day.

And while there is always something new (so far), most of even the new stuff isn't really all that new after you have been doing the old stuff for a while. The incremental improvement process tends to reach an equilibrium state where all you end up doing is adding new details for more and more rare events.

So the work becomes drudgery, for those who have done it for a long time. And that's why we bring in new people to do the old jobs and learn how it works and improve it and adapt it to the new world as it emerges. And those of us who have checked that box a few hundred or thousand times go on to do the next thing, and the next thing, and the next. So we move one!

### Conclusions

Getting to managed maturity in a cyber-security program is not all that hard to so, but at scale it does take time. The reward is fewer (or no) emergencies, reduced cost and increased performance (at scale), more people over time who can do the jobs, and less time and effort in bringing in new people while advancing more experienced folks to do the next thing.

However, as your program matures, it does have a tendency to lose the excitement of real-time outages with consequences that get the CEO out of bed and the investors concerned.

So if you want help maturing your program and making it boring, we can help you there. But if you want excitement and uncertainty, stay at the None or Initial maturity level. It's exciting!

  