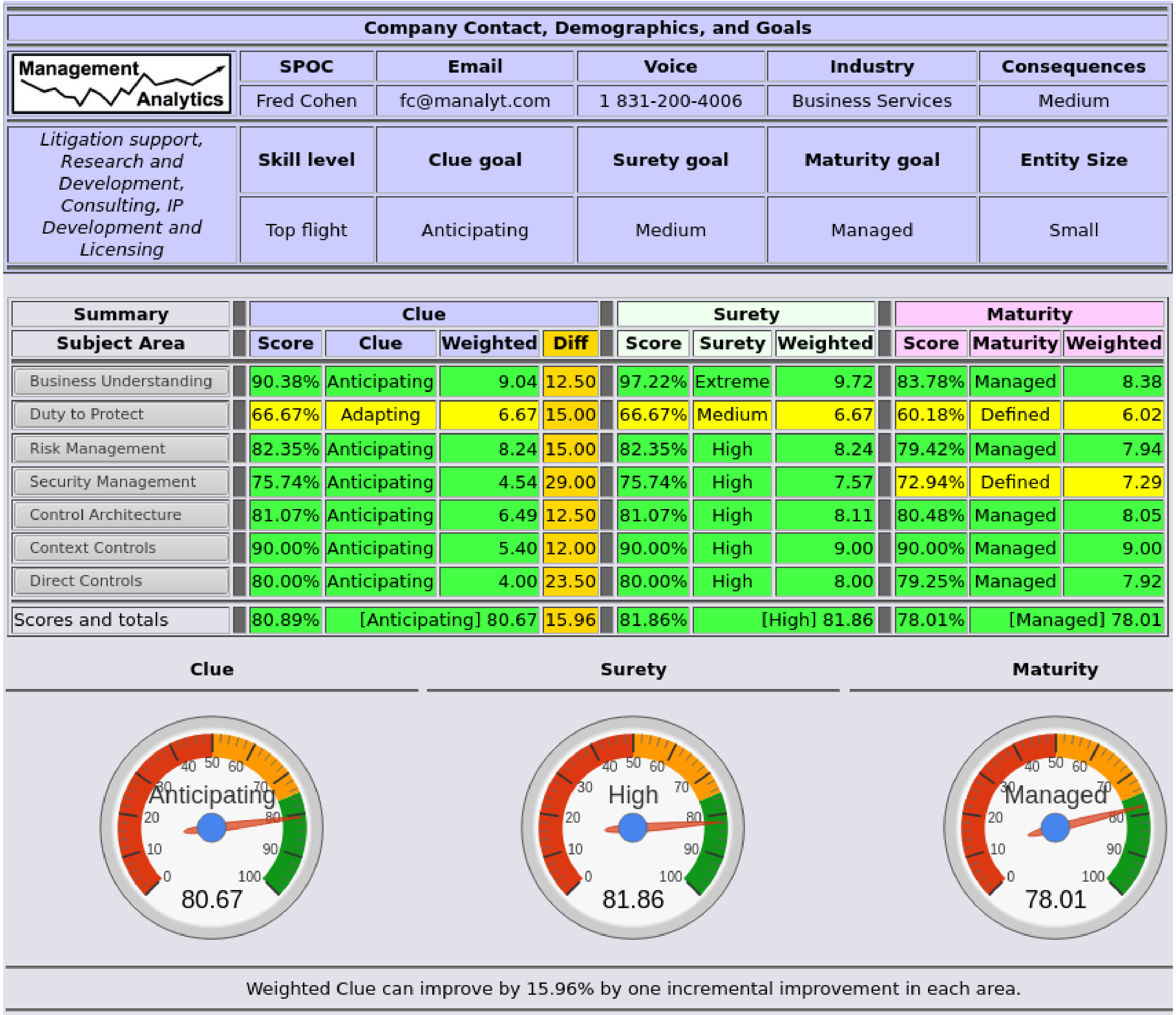
All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Gwiz™ What do we measure and why?

We have been working on ways to measure cyber security since the 1980s and I am certain others have been trying to do this for far longer. This is what we are currently looking at – at the top level – and why.



Company Contact, Demographics, and Goals

Management Analytics	SPOC	Email	Voice	Industry	Consequences
	Fred Cohen	fc@manalyt.com	1 831-200-4006	Business Services	Medium
Litigation support, Research and Development, Consulting, IP Development and Licensing	Skill level	Clue goal	Surety goal	Maturity goal	Entity Size
	Top flight	Anticipating	Medium	Managed	Small

Summary	Clue				Surety			Maturity		
Subject Area	Score	Clue	Weighted	Diff	Score	Surety	Weighted	Score	Maturity	Weighted
Business Understanding	90.38%	Anticipating	9.04	12.50	97.22%	Extreme	9.72	83.78%	Managed	8.38
Duty to Protect	66.67%	Adapting	6.67	15.00	66.67%	Medium	6.67	60.18%	Defined	6.02
Risk Management	82.35%	Anticipating	8.24	15.00	82.35%	High	8.24	79.42%	Managed	7.94
Security Management	75.74%	Anticipating	4.54	29.00	75.74%	High	7.57	72.94%	Defined	7.29
Control Architecture	81.07%	Anticipating	6.49	12.50	81.07%	High	8.11	80.48%	Managed	8.05
Context Controls	90.00%	Anticipating	5.40	12.00	90.00%	High	9.00	90.00%	Managed	9.00
Direct Controls	80.00%	Anticipating	4.00	23.50	80.00%	High	8.00	79.25%	Managed	7.92
Scores and totals	80.89%	[Anticipating] 80.67		15.96	81.86%	[High] 81.86		78.01%	[Managed] 78.01	

Clue — Anticipating 80.67

Surety — High 81.86

Maturity — Managed 78.01

Weighted Clue can improve by 15.96% by one incremental improvement in each area.

***GWiz™** The Governance Wizards – Roll-up of Management Analytics*

The three key outputs are Clue, Surety, and Maturity. And the goal is to have Clue at a level appropriate to the need, surety at least as high as consequences, and maturity adequate for the size and consequence of the entity. But of course you want to know a bit more…

Clue, and in “haven’t got a”

The dimension of clue ranges from none (sleeping) to noticing, responding, adapting, anticipating, and to constraining. Without a clue, you don’t even know what you might notice. When you start to notice things you start to be aware that things might go wrong. When you notice things, you might then start to respond to the things you notice, and from there, using a feedback mechanisms, you might reasonably adapt to the things you notice. After you start to do that and get aware of the bigger picture and historical information, you might then start to anticipate what might happen, and of course once you do that you can start to try to constrain the futures to desired one. They you are doing what we call model-based situation anticipation and constraint. This is what a well-developed security brain does.

Surety, and matching it to consequences

The reality of cyber security for now is that you don’t get to tune an infinite dial from nothing to some maximum in real time. In most cases, when you provide protective mechanisms you are choosing from a finite number of options and you can change your mind quickly, but not the mechanisms you use. So surety ranges from none, to low, medium, high, and extreme, and there are relatively few things that operate effectively as you go up the scale. With no surety, anything can happen, and with extreme surety, you can be very certain that certain things will or will not happen. In between, you go from less certain to more certain that the system works as designed, implemented, and operated.

Maturity, as in “stuff happens”

Whenever you do things and work at getting better at it, you go from never having done them (none) to doing them a first time (initial), to doing them repeatedly with the same things producing the same (or close enough) results (repeatable). Then you may start to document them and understand why they do what they do (defined), start to measure what they do and adapt them over time to reflect changes in the mechanisms and the outside world (managed), and if you try really hard, you can figure out ways to optimize them (optimizing), but be careful that you don’t make them so efficient that you lose effectiveness and make the system brittle. Optimize for what has to be answered as part of that step in the process.

Measured across what things?

We use out standards of practice and the notion of the “security brain” to identify the 7 areas we consider. Business understanding (how the business/entity works and what you are trying to achieve), oversight which defines the duties to protect, risk management (which few people even know the meaning of), security management (the internal governance process surrounding turning risk decisions into execution through the internal control system of management, control architecture (which most people don’t really think about or understand but is the basic models used to make decisions about specifics), context controls (which deal with the different dimensions of situation), and direct controls (the things that sense and actuate the operating mechanisms), those mechanisms being the things that determine the success (or failure) of the business.

Why these things?

Clue is required in order to make reasonable and prudent decisions, and more clue is needed as the consequences go up, because so will the hostility of the environment. In essence, the more you have to lose, the more you have to know what’s going on to keep from losing it.

Surety should go up with consequence because if you put too much weight on something that won’t support that amount of weight, the thing will break. The higher the consequence, the more it will get squeezed to cause the consequence to happen, but more importantly, the less you are willing to have it happen, so the more certain you want to be that it doesn’t.

Maturity is really about the ability to get expected results (at the lower levels), and make sure you keep getting them more right with time and change of circumstance (at the higher levels). If you are in a static situation that will never change, and all you want to do is the same thing you used to do, repeatable is fine, but the world changes, so you need to measure what’s happening in order to tell when it’s going wrong before it does. Otherwise, the repeatability will go down and you will be in the novel situations again and again, requiring extraordinary effort of individuals to keep really bad things from happening. Eventually, all those super duper extraordinary individuals will collapse as will your systems and mechanisms, unless you can mature to the managed level (at least), notice what’s going on before it goes wrong, and act to adapt.

They are related

You may notice that without a clue, you cannot understand enough to know the consequences that could happen to you, and without understanding these consequences, you cannot make reasonable and prudent management decisions. The more clue you have, the more you can understand the consequences of failures, and the more you can work toward a better, more efficient, and more effective set of mechanisms that allow you to match surety to consequence.

So you would expect that for a well-managed entity, these things would rise (and fall) together. In fact, if you are spending a lot on cyber security and not getting the bang for the buck you should be getting, it might be because you are clueless and are spending too much time and effort reaching high levels of surety for consequences that don’t justify it.

When we say reasonable and prudent, that is what we are talking about. Reasonable, as in based on reasoning. Prudent, as in not laughably ridiculous and ignoring what you reasonably should have know. Who could have ever known a backup could be stolen or not work? You now that you’ve read this, and anyone else who has put in a modicum of thought.

And the underlying details?

This is already a 3-page article. You can read through the standards of practice (all.net under Protection) to get a start on the 120 or so different component parts that go with not being unreasonable or imprudent, but really, besides that, if you are going to be a professional (at anything) you probably need to read and understand the field, practice it over time to keep your skills honed, and learn more as you continue to develop. Nobody knows it all, which is why it takes a team to win against another team.

Conclusions

At every level the cyber security brain has to sense what’s going on (i.e., measure something), communicate (the measurement results), decide (typically against a model of some sort), and act (cause an actuator to behave) in order to have functioning system. This article describes a top level set of things to measure regarding governance. And governance is the top-level of the hierarchy of decision-making systems comprising the security brain. Which is why we call the people who do this the ***G***overnance ***Wiz***ards ... ***GWiz***™!