All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Cybersecurity From Scratch – Part 1: The startup

Every once in a while we get to work with a company to create a cyber-security program from scratch. This is called eating your own dog food. The advice we give companies is usually something we help them with, but don't end up having to do ourselves. But in this case...

I am the Interim CIO

As a consultant, I don't take fiduciary responsibility and I am not an officer in any company other than my own. But in this rare case, for the beginning of systematic approaches to running an early stage startup spin-off from an R&D firm, I am acting as an advisor/CIO to a company that I just completed a Cybersecurity Pathfinder for. So…

I cannot also act like a CISO

Separation of duties demands that I cannot specify, verify, and execute the same responsibility if the consequences to the company are high. This is in the Standards of Practice[1]. And according to the analysis at hand, the CISO will specify and verify security issues and the CIO will execute them… along with the rest of the IT everything. So the company decided to do a Pathkeeper to keep us on the cybersecurity path and that is being run by one of our consultants that does that, while I am acting as CIO for a brief period of getting everything going.

Did I mention the other companies?

So as an advisor to the head of the larger enterprise, it turns out there are three small early stage companies that share a lot of characteristics, including largely identical ownership (at inception – investment is changing that, but…). It has become clear that all three of these companies are more or less the same at this point from an IT perspective. So they have temporarily decided to join the planning as a group (sort of like any group of companies with a holding company in charge) and execute independently.

From scratch

Today, there is one worker who does IT for the company. A relatively young recent graduate from computer science school with a good set of basic skills, an interest in learning, and a capacity to take on serious tasks. With no corporate experience, there is no bias against moving forward quickly, and also no experience with all the politics and other impediments to progress. This of course comes with a lack of in-depth knowledge of all the myriad things that can go wrong. There are a few workers with their own computers doing the work, all from home, and a few outsourced folks in a small business with unknown everything, doing it from a small office. They use outsourced email, Web services, and file services. They are working successfully, have adequate funding to proceed, but no real plan for IT. The Pathfinder gave them a cybersecurity framework to work from, so we decided to build it from scratch to meet the framework, and incorporate the IT things we do using the same mechanisms.

1 See http://all.net/ under Protection for details of the Standards of Practice and relevant additional material for this series, including other referenced decisions and terminology, and other identified component parts.

The first decisions

The Pathfinder identified a benefit associated with using remote desktop where feasible to allow for control over protection and configuration management, automated corporate backups, change control, and other such things. It also identified:

- Medium consequences for at least the first 6 months.
- The size is Micro – going on Small
- The maturity of the entity is None and Initial
- The skill level (for IT) is High to Extreme (for our advisors) and Low (for the other folks)
- The duty to protect is not yet defined, nor are policies, procedures, etc.
- There is an urgent need for initial cybersecurity basics training for their current situation
- There is a 6-month time window identified for reaching Defined maturity

More details will follow, but for now, the first IT projects are:

- Do initial awareness training for critical issues (doing backups to a common repository and other contractually mandated items not yet known)
- Get remote desktop working where feasible.

Inventory, work flows, and metadata

Following the Standards of Practice, and trying to get to Defined maturity, Medium surety (matched to the consequence level for now), we will ultimately need an inventory, workflows, and metadata set for running the protection process, so for the first project, I identified that we should create the initial inventory first. We have very little actual hardware, software, people, and content, and setting up an inventory database to meet the relevant parts of the COP table should be easy enough, the IT person knows how to do this, so why not just get it set up and use it to manage the effort to use remote desktop?

Documentation, Procedures, Personnel, Lifecycles, Versioning, etc.

This will also start the documentation aspects of the company from an IT perspective, so why not create the initial documents for each of the inventory items containing the elements of their lifecycles as the structure of the inventory documents? While we are at it, the filenames have been structured in a directory compatible with the inventory approach, and indicate dates and times (sorted by string or number identically – YYYY-MM-DD) so each time a document is edited, it is saved as a new version, with a new name every day.

Identification, authentication, and authorization, use control, and more...

Their email service provider allows multi-factor authentication. Since email addresses are used as identifiers in many such systems, we will go with that for now for identifiers, and then use multi-factor authentication per the Standards of Practice for Medium surety. Problem solved before bothering to worry about it – by using what already exists in a convenient way. Authorization will be a bit trickier, but for now, read only for specification and verification, read-write for execution, and only one person doing the execution, so a risk accepted to create an initial capability. Until the capability is put into use, no substantial consequences other than minimal waste are involved.

Timeline

These efforts are simple to do if you start from scratch, because there is little data involved. Build a database with some number of tables and well-defined columns, build a directory structure and some file templates, and do some simple documentation of what is. It takes a few days for one person who has no group processes to deal with and can simply make decisions.

Decision-related documentation

Very soon, as soon as the documentation starts operating, a set of decision documents will be created to codify decisions and have them properly approved. In the meanwhile, the CISO efforts (currently operated by the Pathkeeper alone) will document the process and related decisions by using the existing mechanisms of the pathfinder, which includes systems of record for taking notes, metrics for tracking the governance process, and the living document that is the Pathfinder As-Is report. When a change is made, the process is tracked in the "Gigs" software we use to track activities and time frames, the AsIs document is changed to reflect the new current situation, and the GWiz™ metrics are updated when the change is significant enough to make a measurable difference in program maturity.

Workflows

As soon as more systematic approaches are codified, they will be turned into checklists for initial procedures, and the structure of the checklists will provide a very rudimentary work flow system, along with the Gigs tracking. A future project for the company is a workflow system needed for tracking compliance requirements, so as that comes online, it will become the operational mechanisms going forward, but you need to start somewhere, so this is a bootstrap effort.

What's next?

In the big picture, a consultant is not a CIO, and the object of this effort is to get things into good enough shape to hand it off to a real CIO as soon as the company gets to a size adequate to do so. Perhaps the current IT worker will be a good CIO, or who knows what? But the goal for setting up the program is to get as far as we can as fast as we can with minimal change and effort, toward the 6-month goal of Medium surety Defined maturity and an operationally efficient and effective IT capability.

There are 122 items in the current list of areas to address in the security path, and operational needs for the IT requirements that have to come with them. Perhaps 20-30 of the security issues are being addressed in the things we are doing now, and the key IT projects are getting started in an integrated fashion. Over the coming week or two, we will sort out the timelines for addressing the 122 items, and at the same time, we will get the urgent things done in the next 10 days, on a preliminary estimated basis. That will get us to Initial maturity on a lot of things, and that will become repeatable as soon as we start to repeat it, then documented as soon as we get it codified in procedures and processes.

Conclusions

This is the first article in this series. The idea is to track what we do and tell you, our readers how we do it as we do it. We will tell you about problems and solutions along the way, at a high level, and keep the company name confidential, as is our tradition… See you soon.

