All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Cybersecurity From Scratch – Part 7: Whatever happened to Part 6?

Every once in a while we get to create a cyber-security program from scratch. …

Last week we should have put out Part 6… but it didn't happen because lots of other things didn't happen… And that's what happens.

- The CEO had pressing meetings.
- The IT director is no longer the IT director.
- And other stuff too long to list here.

So here we are in part 7 – or more specifically, Week 7.

- The CEO decided to accept the risk of conflict of interest between specification and operation of the IT and security functions so we could make rapid progress and meet urgent needs. This was identified and accepted as a risk by the CEO during the weekly Pathfinder.
- As a result, a lot of progress was made on the implementation of technical mechanisms to support governance process. Specifically:
  - A security inventory system was put in place and users were briefed on providing an initial inventory. 25% of the user base has no provided initial inventory information on what cybernetic mechanisms they use and depend on for doing their jobs. The rest are expected to provide information in the next few days, and this an initial inventory from the user standpoint will be in place and reconcilable to the initial inventory of the Pathfinder. This will then link to additional items in the consequences review and allow for linkage of consequences to inventory items and matching of surety to consequence for effective risk mitigation decision-making. It will also establish, in part, the trust relationships.
  - An initial briefing and booklet for security awareness was generated from a previously existing template[1], checked with the CEO and approved for distribution, then distributed to the user base in the weekly group LOR. They are responsible to read it but were also briefed on it. This will be turned into a series of short videos someday soon, and then updates will also be provided as updated booklets (PDFs) and updated/added videos. This meets the initial briefing requirement approved by the CEO and we have scheduled for a monthly update (3rd Friday of the month?) during the weekly LOR.
  - The inventory also includes lifecycle information and is the start of the basis for standardized engineering and corporate document formats – which will come soon.
  - Backups were requested of all team members, as an initial process using an existing corporate Dropbox account for each. This to meet the immediate need only and to get a baseline for size, type, and content they deem relevant.

1 http://all.net/ → Books → Security Awareness Basics

New decisions

This week, in addition to approving all of the previous decisions formally, a set of additional decisions were made and placed into the approval process for formal approval by the CEO after oral approval during the weekly Pathkeeper call. Specifically:

- **Outsourcing people:** For emergence, the situation will likely remain flexible, but outsourced workers should have the same requirements as internal workers for cyber-security requirements.
- **Authentication:** 2-factor authentication using Google's authenticator was adopted as the minimum requirement. Implementation will proceed as operations is able to carry it out. It is already in place for select services.
- **Business Dependencies:** There is an identified need for an inter-dependency model to be sure the company understands what depends on what. As an example, there was discussion on DropBox vs. Google Drive regarding backup and recovery processes and AWS as a service provider for those functions. There is an identified need a data retention and retrieval methodology (the requirements will be detailed in further decisions but a methodology is required ASAP to avoid a variety of potential pitfalls in the short term). The advantage of AWS for this company is that is is an independent, different provider, which is important for meeting physical distance and separate and different requirements for reliable backup and recover at the size and nature of this company. This also needs to be mapped into overall system dependencies and determine whether and to what extent this impacts all three of the current entities.
    - Note - because there are 3 companies and requirements for arms length in some (or most) things, each company should have their 'own sets of things' to support autonomy, divestiture, etc. This is a common challenge to be met by holding companies with subsidiaries, joint ventures, and similar corporate structures.
- **Duties analysis:** While the proposed future state was "External specialists should create and periodically reassess duties to protect.", this is being attempted internally by corporate counsel. Which leads us to…
- **Duties Defined:** Company has decided to create duties to protect using corporate counsel to undertake the activity, and to store them in a database for use by workers. However, this has not yet been done. Without defined duties, making decisions about what to protect how well becomes problematic in the specific sense. As a result, a tentative Duties to Protect will be (we imagine) codified into a new database and updated over time to reflect duties as they are identified. This has to be discussed with e CEO in order to create an initial set of duties in the interim. This has to include codifying regulatory requirements and other things we 'happen to know about'. In the me3anwhile, we are proceeding with reasonable and prudent future state work making possibly incorrect assumptions along the way.
- **Business Model:** No change is anticipated, sort of. For some time the existing model and system of modeling will do. But the business is changing rapidly because of pivots associated with different successes occurring along the way.

- **Content and Consequences:** A process should be started to regularize consequence analysis. In particular, this should be made part of the change control process so that as things change, previously unidentified consequences and consequences associated with changes are identified. Since things are already changing, this is being done along the way through recognition, for example, of new items in the inventory not previously considered in consequence analysis. As they are identified, they are entered into the consequence analysis and documented version of consequences, and if there are changes, they are then reflected across the spectrum of effected components. This process is already underway in an informal way be the Pathkeeper keeping track, but will be moved into a standardized approach over the coming month(s).
- **Scope** has changed informally to all of the IT technology at all 3 companies, and possible new companies are being identified and added over time based on expansion of the company. The CEOs of the 3 companies are approving this scope definition.
- **Separation of duties:** Acceptance of the future state took place (i.e., the same person cannot execute any cyber function if they specify or verify it). However, this was bypassed for the next 3 months to allow the initial system to be put in place using me as the CIO and doing execution.
- **Risk assessment:** Medium threat and Medium consequence will be assumed for the first 6 months of operation. This requires 6 month review and “manage carefully”, “sound change control”, “accreditation processes”, “managed configurations”, “Defined or higher maturity”, and “systematic change management”.

A set of about 15 decisions were delayed until later dates based on the program needing to progress a bit before these decisions could be implemented, and the need to clarify architectural decisions before making these decisions formal (or deciding not to). This was expected because the initial version of timing for reviewing and invoking decisions depends heavily on the specific circumstances of each company. Thus the standard allocated of dates to activities is designed with the purpose of giving a starting point intended to be updated in this fashion.

Roll-up

In total then, there are about 40 decisions made, and 80 to go, (2 in 6) and we are just under 2 months into the 6 month program of getting to Defined maturity. In other words, right on time… In fact, according to the GWiz™ review as updated we are slightly ahead of schedule. But don’t imagine we will keep this up.

The major challenge now is that, while we are catching up on governance implementation, we remain behind on implementing the execution architecture for IT that will allow the security architecture to meaningfully function. While we hope to catch up soon, it will likely be at least a month before this happens, and that assumes more changes and surprises don’t happen. Which of course they will...

Conclusions

The process is operating as it should, and even though the implementation of the IT components is slower than desired, governance is being put in place and executed upon. It will take some time for things to become regularized, properly documented, and properly operational for scaling, the next challenge.

Additional Capabilities

Because Company was unable to rapidly implement certain things, we used our systems of records (JDM and Gigs) to quickly implement interim solutions. These solutions include:

- **Inventory for security (and IT)**
  - Inventory was a pretty simple thing to put in place. We decided to implement inventory for now on a per person basis, because that's how information came available to us. So each individual has an inventory of the items they operate or need to operate. Here is sample output from one of the users:

Item 1020	iPad Pro (personal)	Personal	System	Unknown	Operation	Technology	Critical infra	[Link]	Sat 2021-05-22
Item 1030	U-Verse 1,000 Mbps High-Speed Internet	Personal	System	Connectivity	Operation	Technology	Critical infra	[Link]	Sat 2021-05-22
Item 1040	Orbi Router with 2 Satellite Units spread around the house	Personal	System	Connectivity	Operation	Technology	Physical plant	[Link]	Sat 2021-05-22
Item 1050	HP OfficeJet 5200 Series Printer (personal)	Personal	System	Unknown	Operation	Technology	Physical plant	[Link]	Sat 2021-05-22

  - This example is the preliminary input, sent back to the user for confirmation and additional information. For example, this home-based user has high speed Internet that they currently pay for, used for connectivity, part of operations, a technology component, and dependent on critical infrastructure (in this case the Internet, power, etc.). A personal iPad Pro is in use, for unknown purposes, which has to be updated by the user to clarify the business utility (and thereby the associated consequences of protection failures). As a starting point, this will get things going, and additional fields can be added as/if required, as well as export, etc. when a new database approach is put in place.
- **Additional linkages**
  - For efficiency reasons, we added linkages between elements of GWiz™, Gigs, and JDM. The links field identified in the inventory allows linkage to other elements of the Standards or Practice, Risk management decision documents, or whatever else may be desired. As an example, the backups for each system might be linked to the inventory to allow content to be examined and restored, preserved, etc.
  - Links can be very useful, but they can also be problematic, in that they allow easy distraction, and place a high dependency on stable naming and location information. Nevertheless, the convenience provides a useful way to quickly find what is sought, and eliminate many steps in processes.
- **Sorting by last change**
  - An interesting side effect of this example pathfinder was the utility of "last changed" information. The systems of records we use are very handy for moving forward quickly with sets of things to get done, but not so good at recalling what you just did. The information is in there, but picking it out and using it for various purposes may be more complicated because of all the historical information involved. We added a function to permit sorting Gig entries by last save time. The net effect is that during client meetings, rapid progress may be made, and after the meeting, last change information can be used to recall all of the things done and perform related information, like updating GWiz™ data, updating or adding formal decisions to JDM, and so forth. Last change information, for example, made this report far easier to write, and I had not problem remembering what was done.

