All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Cybersecurity From Scratch – Part 5: Starting to rock – but for a role!

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

The process of decision-making and approval is now pretty solid. The CEO is working through the 120+ decisions about future state over the next 6 months at a good pace, asking good questions and getting answers, spending an hour a week on the process.

New decisions

This week, in addition to approving all of the previous decisions formally, the cybersecurity management "Who does it and where are they placed", was accepted per the reasonable and prudent future state, as was:

- Separation of duties
  - The current challenge of separation of duties is the very limited staff. An additional execution resource has been identified as needed and outsourcing is required in order to implement the remote desktop / Apple endpoint solution already in process. Other internal progress is slower than anticipated, owing in part to COVID vaccination processes and their temporary effect on workers after the 2nd dose.
- Risk aggregation
  - The SoP future state of "Client should fully integrate risk aggregation and interdependency into operations and change management practices." was adopted, and is relatively simple at this point because the change control management scheme is not yet fully in place. It is, however, operating, in the sense that the change of scope drove a need to review new system types for risk-related issues (pending a scheduled activity) which will trigger the other changes associated with the results, whatever they may be.
- Risk treatment
  - The SoP approach to risk treatment was reviewed and accepted, and is rarely considered controversial, as it is largely a logical application of the meaning of the options (avoid, transfer, accept, mitigate).
- Initial identified threat set
  - The following were identified for the consequence levels assumed based on the SoP and Client identified threats and history: activists | club initiates | competitors | consultants | crackers | crackers for hire | customers | cyber-gangs | deranged people | drug cartels | economic rivals | extortionists | spies | fraudsters | global coalitions | government agencies | hackers | hoodlums | industrial espionage | information warriors | infrastructure warriors | insiders | maintenance people | military organizations | nature | organized crime | paramilitary groups | police | private investigators | professional thieves | reporters | terrorists | tiger teams | vandals | vendors | whistle blowers

- Risk assessment process
  - A Pathfinder/Pathkeeper fully reviewed every 6 months was selected out of the available medium consequence and threat arena, and of course it has already been adopted and is underway. At this time, it is expected that a rolling process of review will take place, this the question of whether a full pathfinder review will be done separately is in question. The Pathkeeper is updating the metrics program along the way, and the As-IS state is also being updated through the Pathkeeper, but as and if Defined maturity is actually reached, some decisions about moving to Managed maturity will have to be made, and these decisions will depend to a great extent on the progress of the company over that time frame.
  - Sound change control will likely be partially adopted for cloud-based remote desktop systems and other such systems, however, at the operating system level, commodity operating environment updates will likely be used off-the-shelf with only operational testing of patches and updates prior to deployment (to avoid failures with software and setup and avoid disrupting normal operations). A roll-back capability will likely be used and a backup and recover process was also identified as part of this requirement.
  - Careful management implies substantial attention, but not continuous security focus as would be required for higher consequences. The weekly review process for the CIO to keep security as a priority is effectively helping to meet this requirement.
  - Accreditation processes are required for the deliverables of the company, and an accreditation process is readily feasible for configurations of the system (Apple endpoints and tightly manged remote desktop servers), as provided by existing 3rd party vendors such as IBM. This will afford a high enough level of surety and releive internal efforts for dealing with security issues in these systems most of the time.
  - Configuration management is detailed in other SoP future state recommendations, all of which appear at this time to be achievable with standard application of high quality specialized vendor solutions.
  - Maturity Defined or higher is ultimately desired/required, and the current process is aiming at Defined maturity in 6 months (now more than one month in). The ultimate aim is Managed maturity after Defined is reached and found to be operable within defined business requirements.
- Risk management approach
  - The SoP risk management approach was accepted with expectation of implementation to the Defined maturity level within 6 months. At that time, there should be enough information in place to make reasonable and prudent decisions as the next step in the program is started. It is important to note that the risk management process will remain an approximation for some time to come, because a duty to protect analysis has not yet been completed, and until it is, there is nothing to drive the risk management process other than the SoP initial Pathfinder decisions. These are reasonable, except of course that they require Duty to Protect analysis be completed to make certain all required duties are met, unnecessary excessive protection is not used, and management roles are proper.

- Business dependencies
  - The need for a model was agreed to and a model is scheduled to be developed over the coming months as the IT infrastructure is built out. The modeling framework suggested by the SoP future state was tentatively accepted as a starting point. However, this is likely to change as a business-specific model is developed.
- Business model
  - The existing model of the business is changing so quickly that further formalizing it at this time would be wasteful, so the existing (changing) model was adopted for the next 6 months. As the business model is developed, the dependency model will be develop din concert and drive the need for surety in mechanisms that are dependent on for higher consequences than they would normally encounter.

The “How does the manager mange…” question was put off (i.e., the risk of not making the decision was accepted) for 4 months because of the rapid changes underway and the current lack of anyone to manage for the identified functions. The Threat assessment process was delayed by 2 months because it is complex and takes time that would slow other efforts (based on the acting CIO’s recommendation).

Roll-up

In total then, there are about 20 decisions made, and 100 to go, (1 in 6) and we are just over 1 month into the 6 month program of getting to Defined maturity. In other words, right on time… but don’t count on it...

The major challenge now is that, even as we make these decisions, we are falling behind on implementation. This is because of a resource limitation owing to the early stage of the company. This is well known to the CEO who is addressing these needs along with the CIO, but will necessarily delay some of the implementation.

Having said this, the current plan is achievable, but at some point, one or more of these things is likely to happen:

- The plan and process will be slowed down and not meet the 6-month goal of reaching Defined maturity.
- Additional internal resources will be brought to bear as and if funding becomes available and operational personnel are identified and hired.
- Additional external resources are engaged.

The major problem today is that an internal resource has to be put in place to effectively manage the external resources, or the separation of duties requirements just approved will have to be waived for a period of time for the purpose of allowing the specification and execution of the program to be done by the same person or people. None of these are problematic in a serious way for a company in this stage, but all depend on resources that are not always easily attained in a startup situation.

Conclusions

The top management decision process is effective, and good decisions are being made with adequate information to make them. But we need effective execution to proceed at speed.

