All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Cybersecurity From Scratch – Part 2: First Decisions

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

The first decisions are often the most consequential, but most of them can be made very quickly if you are in an early stage. A Pathfinder having been done, the first thing to do in a startup situation is to get decisions on the easy stuff. Things like risk definition, the future of outsourcing, consulting, the form of duties, the knowledge program, organizational structure, mobility, scope, and so forth are largely acceptable quickly.

The meeting

A live online remote (LOR) call with the CEO, CIO, IT director, and Pathkeeper Lead took about 30 minutes to go through the initial decisions. All were reviewed, discussed briefly, and being as the CEO had already read the Pathfinder report, about 15 decisions (out of 120) we made on the spot. These decisions were codified using the Gigs and GWiz™ software packages during the call, with follow-ups scheduled for the next weekly call for signatures. The IT director had not yet created the decision documents for signature, and thus separately documented approval in the document management system had to wait (for the document as well as the document management system to be in place), but in the meanwhile ...

The approval process

A decision was made during the LOR to allow the approval process to work as follows:

- The parties know each other by face, voice, and limited history
- During a LOR call, when reviewing a decision, an oral agreement by the CEO is adequate to activate the decision.
- It is codified on the screen live and saved in a system of records (Gigs) so that the CEO can see it as it is codified.
- A formal decision document will be created after the meeting for signature by email “Yes” using the internal email system.
- An email at the end of the meeting demonstrating the decisions for all is sent, and later the details are updated in JDM and GWiz™.
- The internal email system was approved for exchanges of Medium consequence or lower, which essentially all of the decisions are.

The beauty here is that no written signatures or “ducusign-like” mechanism is needed. The decision is made and codified in front of all, stored in a system of records (effectively append only from the user perspective), and a formal documentation of it is put in the repository (database pointing to file server). The CEO has agreed and there is no obvious residual risk other than some sort of attack on all of these independent systems run by independent parties, and even if someone wanted to disclaim it, the others would say – no!

 Copyright (c) Fred Cohen, 2021 - All Rights Reserved

The decisions themselves

Risk definition was adopted from the Pathfinder – in this case, a 2-level (Critical / Other) model was used with definitions combined from typical 3-level definitions. This for simplicity of early implementation and with the idea of going to a 3-level version over time (the 6-month revisit time – not yet approved but recommended pending approval).

The future of outsourcing was adopted from the Pathfinder SoP with a minor modification by the CEO. In essence mostly outsourcing, protected as well as non-outsourced similar things.

The future of consulting was more or less unchanged except for controls identified elsewhere.

The form of duties was identified per the SoP as an enterprise database, which is already being formed for inventory and incorporating metadata and lifecycle needs via standard inventory documents and fields.

The knowledge program is at its beginnings, and while the general form is not yet formally approved, there is an urgent need for initial awareness training, that is being worked, but cannot be delivered quite yet because the decisions needed to do it have not been made. We used an existing awareness document that I have published, authorized extraction of relevant parts for an initial training basis, it will be formed and approved in a week (selective copy and paste we hope), augmented with specifics we have identified to date, and a short video will be made to train it. The video and resulting document will be made available to the team via Google drive invitation with a simple Google form used to generate demonstrations that they read/watched and know the right answers. That will do for the first training session, and a month later, an improvement/update will be required according to the initial (not yet approved) retraining requirements.

Organizational structure and mobility will remain unchanged, so that was documented.

Scope was changed to the conglomerate this company was part of (3 small companies) with largely identical everything. We are initiating meetings with the CEOs of all three next week, and off to the races for all three of them… we hope.

GWiz™ update

Updates from the meeting were put into GWiz™ to reflect the changes, changing the overall Clue rating from somewhere under 5% to almost 13%. The goal is 50% (to reach Defined maturity) by 6 months, and progress is now ahead of time frame to achieve this. Warning – the easy stuff is first and fastest – things will slow down...

What’s next?

There are 122 items in the current list of areas to address, and we have identified 25 items for the next meeting, of which 8 are simply confirming the written approval of the decisions now in place. At that point, those 8 items will be cycled for revisit in 6 months (per the re-visitation time on decisions in Medium consequence situations of the SoP produced by the Pathfinder). The 17 remaining items are scheduled for discussion next week, most to be approved or changed at the CEO’s discretion, and each leading to

Conclusions

So far so good… that’s what the man who jumped out of a 50th floor window of a skyscraper was heard to say passing the 37th floor… See you soon…

 Copyright (c) Fred Cohen, 2021 - All Rights Reserved

Terms and tools used:

Some of the terms and tools identified above represent pretty complex stuff, so I thought I would add some details here at the end.

- **SoP:** Standards of Practice, a set of long (now) published but constantly adapted strategic decisions on cyber-security published at http://all.net/ under Protection. Each decision has:
  - **Decision name / Question:** This is the name of the decision, but is generally formed as a question, such as “How do you analyze threats?”
  - **Options:** This is a finite list of alternative answers to the question. These are decisions of kind, not decisions of amount, although they often indicate amounts associated with the kinds, such as associating a risk acceptance period associated with a consequence level.
  - **Basis:** The reasoning behind the decision. This can be used for justification, but it also introduces the limitations of the decision, which is meant to be adjusted by a knowledgeable expert in conjunction with the decision-maker.
  - **Decision:** This is the selection of one or more alternatives in the context of the situation at hand. For example, different decisions (choices from among the alternatives) apply for different sizes, maturity, consequence levels, etc.

    Again, this is intended for use with experts and others who might identify new alternatives or other approaches. As we operate the SoP over time, we update by adding new options, new analysis in the basis, and changing the decision for other reasons, such as changes in the external environment of the cyber-world.
- P**athfinder:** This is a standard process based on applying the SoP. It consists of
  - Identifying the current situation based on what the client says, typically without any attempt to verify the claims, which we have found to be counterproductive.
  - Presenting a reasonable and prudent future state based on the SoP and a time frame to move toward that state.

    Note that this is NOT THE ONLY reasonable and prudent future state. It’s just an example of one. Thus the entity must make decisions that may still be reasonable and prudent even though they are not those identified by the SoP, and of course they should then justify them with their own basis
- **Pathkeeper:** Once you do a Pathfinder, a Pathkeeper is used to keep you on the path toward the reasonable and prudent future state. In essence, you get ongoing advice, typically weekly, with a monthly advisory board meeting, to help you figure out how to execute on the path, to adapt as you make decisions, and to update the “reasonable and prudent” future state with the new basis and decisions.
- **Gigs:** This is a tool we use to track what we do and are planning to do over time. It is a system of records, so it never forgets anything (normally), and it creates, by the user using it, contemporaneous records of planning and execution over time, keeping everything and everyone up to date as you move from here to there.

 Copyright (c) Fred Cohen, 2021 - All Rights Reserved

- **GWiz™:** The Governance Wizard (in this context) is used to put metrics on the state over time, and to measure progress from the initial situation through today. It rates strategic decisions in three areas (not orthogonal dimensions), in the case of a Pathkeeper, being Clue, Surety, and Maturity. As the program progresses (we hope) clue increases (you start to get a clue) as does surety and maturity. The Pathfinder normally identifies a desired maturity and surety level (the surety matches the consequence from risk management decisions, and the maturity is determined from the surety requirements). GWiz™ also provides linkage between the metrics and the JDM decisions, and a connection to Decider™. GWiz™ also provides automated analysis that identifies (and sorts from best to worst) the next best thing to do to improve your clue (and with it your surety and maturity). Note that this analysis is purely based on the resulting improvement in your measured levels, and doesn't in any way reflect on what you might think is more or less important.
- **JDM:** Judgment and Decision-Making is designed to support decisions of the sort (strategic, not real-time time frames, between finite options, etc.) of the SoP. In implementation, it is customized to the SoP so that the reasonable and prudent future state analysis from the SoP is largely automated, and even when not, it supports the analyst in making decisions and explaining them efficiently. So after you spend 10-20 years exploring every case, you can do the same analysis with the same results from the same facts reliably, and then adjust the decision for the more nuanced situation of the specific client. It also produces a human-readable report that can be readily searched and selected to get to specifics quickly, assuming you have practiced with it and already know what everything means and how to use it.
- **Decider:** Decider is used, in this context, to prioritize actions. In essence, the GWiz™ results set the favorability of each strategic program element based on the metrics used to rank clue, surety, and maturity, and the human then identifies the importance (to them or the entity), and the result is (after you push the right buttons) a prioritized list of what to do next. Unlike the GWiz™ analysis, this focuses entirely on the decision maker's prioritization combined with the favorability of the situation for each factor in the decision.

Themes in the tools:

You may have noticed that each tool is designed to help human experts make good (usually satisficing) decisions quickly and to document those decisions and their basis rapidly, as they make the decisions, act on them, and adapt them with time. None of the tools force anything on anyone, and the methodology as a whole operates under the assumption that people will make these sorts of decisions, using experts to support their efforts, and the tools will advise, but not decide.

Then who decides?

In our advisor practices, we have a saying:

We advise, You decide

It's generally the CEO or some high level executive that is making the decision for a company about these sorts of strategic issues. The tools just help experts work with responsible people who make and justify reasonable and prudent decisions.

 Copyright (c) Fred Cohen, 2021 - All Rights Reserved