All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Cybersecurity From Scratch – Part 8: To the Control Architecture

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

Management issues were completed to the extent feasible without defined duties to protect, and control architecture was engaged.. In the meanwhile, the discussions surrounding issues got more involved, with the CEO drilling down into the reasons for some of the more complex decisions and, from time to time, starting to execute. Now that the execution has been temporarily enabled over the conflict of interest issues, specification and execution are starting to proceed at a faster pace.

New decisions

Of course formal approval of the previous decisions continued, but the new decisions started to get more interesting. Specifically:

- **Procedures:** The decision was taken to put in place procedures to cover most of the activities by which policies are implemented, protection activities are carried out, and user activities are carried out, and to define and implement them in writing using a workflow system or a fully automated system, with controls to carry them out only by authorized parties, document them as carried out, track, audit, measure, and adapt them over time.
- **Intelligence and counter-intelligence:** The decision was to start with the initial program and augment it over time for higher consequences as the program advances toward Managed maturity (in 6 months or more). This involves, specifically, external influence operations detection, external information sharing access, inbound intelligence defenses, and internal counter-influence operations. In implementation:
  - External influence detection will be based (initially) on Google alerts looking for trade names, company names, and key words associated with the reputation of the company. This was initiated during the decision process.
  - External information sharing is planned to come through the appropriate ISAO as an inbound feeder at the operational management level with upward feed to top executives (per the cybernetic structure of the program to be discussed later).
  - Inbound intelligence defenses will be in the form of an operations security (OPSEC) program to be defined over time, but to start with a review of the existing external interfaces for information derivable about internal operations and awareness. However, until duties to protect are more defined, this program will be limited, and as the inventory system becomes more fully operational and linked to consequence analysis, high consequence outcomes will become the predominant focus of the OPSEC program.
  - Awareness programs will be used for internal counter-influence operations as part of the monthly internal awareness process, and tested at least quarterly as the measurement process.

- **Personnel:** Linkage between personnel and cybersecurity is initially limited because there is no HR department yet. This is planned as an outsourced activity, and as it is rolled out, linkage between HR and other aspects of the architecture and operational design will be integrated. For the short run, the HR department will handle or be involved in all substantial personnel issues, however, the IT Director was terminated before an HR department was in place, so this is still aspirational in nature. Knowledge as shown by qualifications and suitability for tasks will be tracked by HR and used to determine suitability for jobs. This will ultimately end up integrated into identity management, however, this aspect will await completion of Defined maturity where many other aspects will also be put in place.
- **Background checks:** The net effect of this decision is to do background checks using a service through a private investigation agency or law firm. Since duties to protect are not yet defined, the specifics of the checks won't be clear for some time, because adjudication decisions depend on duties and their implementation through risk management. However, all key workers, new workers, and critical function workers will have background checks with updates no less than once per year.
- **Modeling:** The decision was mate that a control architecture should be in place to include at least protection objectives, access control, original identification, identity proofing, authentication, access facilitation, trust models, and change management. Authentication has already been identified as requiring 2-factor for essentially all uses.
- **Control architecture:** Having decided that a control architecture is required, the details are then started through the process, with decisions as follows:
  - **Establishment:** A formally established control architecture for the enterprise will be applied.
  - **Objectives:** Since a portion of an enterprise is highly IT-centric, ratings for Integrity, Availability, Confidentiality, Use control, Accountability, Custody, and Transparency will be associated with groups of content such as databases, files, and/or directories. This ties directly into the security inventory, which includes all of these areas as potential consequences, and ties into the scope of the program, which ties into the consequence analysis already done in the Pathkeeper which includes all of these areas, and which must be updated as inventory changes. As the initial inventory proceeds, additional items will be used to update the rest of this set of items and as/if new requirements are identified they will be managed. But for now, all of the identified inventory items are fitting into the initial Pathfinder with a few exceptions already handled.
  - **Access controls:** The SoP indicated that a subject object model should be used for access control, however, this was because of the small initial size. Rather then redo the decision as the company grows, the analyst suggested going directly to Attribute Based Access Control (ABAC), which is essentially a variation on roles and rules. This will likely also be consistent with existing standards in the area this particular company operates in, so is likely to be compatible with other requirements as they are developed.

- **Original identification:** This is a fairly complex decision reflecting different requirements for different classes of situations, but in essence, the SoP future state recommendation was adopted.
- **Identity proofing:** Again, this is a complex set of requirements, which were adopted, and which is exemplified by Passports or Drivers Licenses combined with a verification check, which is normally required for US employment in any case (to verify a valid SSN and authorization to work).
- **Access facilitation:** In this case, the SoP was adopted and calls for: Unified or Consolidated access, tracking, and use control across enterprises, zones, subzones, applications, and mechanisms at medium or high granularity. This is consistent with the ABAC approach above, and will require an identity management system with provisioning and HR integration for job changes and terminations, onboarding, etc. This also leads to a reduced (nearly single) sign-on approach.

In combination, an architecture is starting to arise along with many of the selections of products and compatibility. The Pathkeeper lead will start looking into specific solution sets that will work with the rest of the environment, and within a few weeks some selection options will be put in place to support the process. Once these are identified and the IT architecture starts to move forward, the integration of other components of the security architecture should be relatively integrated, transparent, automatic, and because of the access facilitation component, it is likely to be easier to more of the functions as the architecture proceeds than it is to do the functions today in the disparate approach resulting from initial actions and natural selection.

In the meanwhile...

Of course this doesn't stop the processes being created for the decisions already made. Documentation standards are starting to emerge, and procedures are starting to be developed, and they will be documented along the way. In essence, the first time something rare (monthly or less), it will be documented and the document only updated as required. This gets to defined maturity as soon as the process is repeated a few times. Activities performed more often will be done repeatedly and adapted till they produce the same results for the same situations again and again, (Repeatable maturity) and then documented the 2nd or 3rd time as they become normalized. An example of this is the processes of the Pathkeeper itself, which are already well documented, and are thus already operating at least at the Defined maturity level. Another example is the approval process for governance, that has now been done 50+ times, and will be put into a written form for future use, ultimately resulting in a checklist of some sort for many situation, except of course the SoP operating through Gigs is already systematized to beyond this point.

In total then, about 50 out of 120 decisions are made, and we are on schedule for Defined Maturity in 6 months if we can get the Duties to Protect defined in time and get the IT functional support process working.

Conclusions

The process is operating better every week as the CEO gets better integrated and starts to see the overall governance perspectives across the company as a whole. The automation is getting more useful and the pace and ease of decisions is improving.

