All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Cybersecurity From Scratch – Part 3: Change happens (quickly and slowly)

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

Things are starting to slow down, and it’s not because the executive isn’t making decisions in a timely fashion. It’s about execution speed.

What now… and next

The conglomerate (small but a group of companies rather than one) has become involved because of the efficiency of working together. Three companies with similar ownership are now joining forces in their cyber-related efforts. As a result, clarity has gone down, thus uncertainty has gone up, thus execution is less certain (to be right) and more certain (to run into bumps). Not exactly a new story.

A new system added

During the past week, a new corporate system was added for regulatory compliance and engineering change control in the form of a quality management system (QMS). Of course the decision was made without consulting security, or telling the interim CIO, but what did you expect. This is reflective of a lack of maturity in the IT Director, and something that the CEO has now asked me to help improve upon. Young companies tend to have young team members, and the lack of maturity of the company is reflected in the lack of maturity of process and team members. The goal of the current cyber-security program (and IT) is to reach Defined maturity in 6 months (5 left). So it is of course to be expected that change not yet under control along with inadequate procedures, training, awareness, etc. which leads to poor and untimely communications, etc.

Which triggered...

During the weekly call, this systemic change was identified, and of course it triggered the “oops” response. Instead of an email between sessions, the new system has to be added to the inventory in JDM, which triggered the need to do the risk review of the new system to identify consequences of failure, and of course this could not be done immediately because of the other things to do on the call. So that was scheduled for the next week. It’s not a hard or complicated thing at this point, but it has to be done and folded into the rest of the systems. So inventory of content changes, consequences change, system types change, and people types change (because the new system has new authorities this of course also changes the actual roles and rules, endpoint / server detection and response, and so forth. On the up side, since these systems are not all yet in place, nothing had to be actually changed (yet).

An endpoint decision

Then there was the decision to go to company-owned devices for endpoints. This instead of every worker using their own computer for everything. Of course we don’t yet know if all of the workers can use Macbook Air as their platform, because some software won’t run the same (or at all) on a Unix platform. But fear not, there is a Windows emulator for Mac… just in case.

This decision is not a hard one to make. Most companies require that you use a company-authorized (and owned is better) system for work. It’s critical to keeping control over the technical controls on endpoints, and the ability to manage things like theft of devices, endpoint settings, plug-ins of new devices like external storage, backups, change of workers, and so forth. The cost is also fairly low. When you look at an employee costing from $60K/y to $250K/y, and the cost of a laptop is $2K for 2 years, it’s a small price to pay. The same is true for Internet connectivity. The company sprung for a high-speed Internet connection for workers who didn’t have one yet, for about $100/mo. So for $3K/y they have assurance of the ability to perform, communicate, work collaboratively, maintain cryptographic controls over work-related activities for distant workers, the ability to do backups and not lose ‘local’ data, and so forth.

Other key decisions

The Standards of Practice protection model was adopted, (signature to be produced as supporting workflow systems come online – they are looking for one...). The scope of the protection program was changed to cover the 3 companies rather than one subsidiary, this effects the hierarchy a bit, but is not systemically impacting on the security issues, the goal of Defined maturity by month 6 was approved, location-based controls were adopted (cryptographicly secured communications, physically secure servers off premise, and secured endpoints for users were approved), duties are being created by insider counsel who is also dealing with regulatory issues in any case, and as developed, they will be added to the inventory. The delay in this of course causes uncertainty and delay in implementation, because you cannot do your duty unless and until you know what that duty is. But practiced hands help here, as the Pathkeeper crew knows pretty much what will and will not pass muster globally, having done it for so many large enterprises before.

But getting it done…

I have heard some people say that making the decision is the hard part. And I have said it from time to time. But in truth, while things get easier from an emotional standpoint once decided, on the ground, it’s a bit different… To quote from Oliver Twist (regarding the laws)

> "If the law supposes that, the law is a ass... If that's the eye of the law, the law is a bachelor; and the worst I wish the law is, that his eye may be opened by experience ... by experience."

Just a simple awareness program...

It’s one thing to say “we decided to do an immediate awareness program”. It’s quite another to actually do it. As simple a task as it seems to tell people what they are supposed to do and not to do, I have a few questions (and answers):

- Without a defined duty to protect, how do we figure out what is supposed to be done and not to be done?
    - *The SoP identifies that for an initial training when no duties to protect are in place, a first step is to teach use policies. These are typically stated on the Web site and can be taught in 15 minutes or less. They can be derived from standard use limits on sites, augmented with the urgent matters identified in the Pathfinder, and put out in a week or two – with an approval for 30 days or so by top management before a revisit. If done well, the workers will know there is more coming.*

  - *For this particular company,we are re-purposing an awareness booklet from all.net (with my permission – under the Books tab on the left); removing what is not needed for now, adding what is needed.*
- Even if we know what to tell them, how do we convey it so they will remember and do or not do it?
  - *I am a fan of multi-modal training and awareness, but again the SoP identifies specific training methods for specific purposes. In this case, they are:*
    - *Upon start of work for anyone: Use initial awareness training.*
      - *And for all current workers as soon as practicable.*
    - *At least once every six months: Use periodic security reminders.*
    - *For personnel with access to medium or high risk systems or content: Use training sessions.*
    - *When periodic (usually monthly) department meetings are held: Department meetings.*
  - *The SoP also provides the following guidance in the basis:*
    - ***Initial awareness training:** Initial briefings are required for all those who access information within an enterprise setting. These briefings lay out the specific things the user has to know in terms that they can act on. Most employees get initial employee briefings through the HR process when they first arrive to start work and this is an ideal place to include the initial information protection briefing.*
    - ***Training sessions:** Training sessions are typically scheduled in groups at a department or similar level (typically 10-30 people) and are carried out by trainers who review specific issues during each session. More effective programs include some sort of feedback to assure that the training is effective at least to the extent of demonstrating knowledge of the content of the session.*
- Even if we convey it, how do we verify that they actually reviewed what we told them?
  - Note the… "*More effective programs include some sort of feedback to assure that the training is effective at least to the extent of demonstrating knowledge of the content of the session.*"
    - In this case, we decided to do a written briefing, a slide deck with audio presentation (5 minutes or less – hopefully 2) for the critical matters. We notify them of it, ask them to review it within a few days, place it on a service provider system (dropbox, Google drive, whatever) and use their mechanisms to verify it was downloaded or viewed. If not, we have to remind them of course… Plan, Do, Check Act – the ISO way…
    - And then we do the quiz – in this case s simple Google form – they are given a URL, have to go answer 4-5 questions (correctly we hope) and we verify it was done and got right answers. Again, we have to Plan, Do, Check, Act.

- Even if we verify that they read/saw/heard/whatever it and understood it, how do we verify that they will/did do it?
  - There lies the rub… which is why we tend to and desire to use automation wherever feasible to do the things required rather than rely on and interrupt people in their work doing these things. A simple example is Backups, which in controlled systems can be fully automated and readily verified. This reduces security load on the users while increasing the reliability of the process. It's better, faster, cheaper, more reliable, and why should people have to do things computers do that well?
- How often do we need to tell them again / make changes?
  - Again, the SoP tells us that for the Medium consequence level, at least once every 6 months is appropriate – but this has not yet been formally adopted.
  - In reality, as things are deployed, there is initial training for each, and the awareness and training increases for each thing people do and work on. This then takes us back to the inventory and change control systems and the roles, rules, and HR interface with identity management. But those are things to be decided in the coming weeks / months...

So much for the simple part...

In execution, these are some of the things identified for the IT director to take into account as the systems are developed (as conveyed orally and now through this document, which the CEO gets before release of course...):

- Each item of content/system/people/businesses should be associated with one of the identified types in the SoP, or we are missing a type.
  - If we are missing a type in JDM, we should identify that, add it, and setup to review the effects and dependencies within 30 days with an exception by the CEO that has to get revisited every 30 days (for high consequences, and since we don't know if the consequences are high until we do the review, that is the scheduling requirement).

  The consequence levels should also map into the JDM consequence levels and be in the database as a field - for each record (as well as for the types).

  - Just part of the update process...

  So the database should have a field associated with those select-able elements, and if there is something that does not fit, we need to update JDM to indicate the new content/ system / people / business type
- Since there is no current engineering change order or similar documentation, something has to be created. Sample engineering change documents from the Web were rapidly garnered (took a minute or three) and used as a starting point… until I found out that a QMS system had been selected. At that point, the QMS system already has a standard approach, which we can immediately adopt. Yay! Of course that has to be reviewed, etc.
  - These documents we are creating also go through the lifecycle process - so drafts to me for review and suggested changes before sending to the CEO and

Pathkeeper for review and feedback. Then we send it to the interim CISO for approval of the form as appropriate, then to me for approval, then approval of the form by the CEO, then put content within the template for the present decisions, they get approved by the CEO in final form, and all of these things go into the storage pointed to by the database for such forms.

- Generally, this process (a draft of it) should be documented as a procedure for creating official corporate documentation.
    - So create the document of the procedures you are using to create the document of the procedure then apply it to the other documents…
        - "It's turtles all the way down…"[1]

The bootstrapping process in general

There are a lot of better and more advanced systems for doing things than my systems. They have great graphical interfaces, they run cleanly for thousands of simultaneous users, they automate standard processes specific to the enterprise, … all that and more. Except they take a few years and a few tens of people to get right for a mature company and to keep up to date as the minor changes take place.

The problem is not so much running a comprehensive protection program once it's in place with enough people to run it and proper controls with auditing, redundancy, management structure, etc. Of course most such programs don't really run right, but that's in no small part because it's very complicated to do well, and repeatable solid people, process, and systems are hard to create and maintain, especially in a world where we value creativity over rote activities.

My systems are all bootstrapping (pulling themselves up by their own bootstraps) all the time. You can't do this right till you do that, but that requires this to be right in order to work. So you do a little of this and a little of that, using experience in place of process to develop process to replace experience.

And you thought building a security program from scratch was going to be boring...

What next?

We don't know yet, of course.

Right now, we have so many things to execute on that we are starting to fall behind. Which is not unusual. No plan survives contact with the enemy.[2] But with no plan, you will not survive contact with the enemy either. So pretty soon I will step in and engage another one of my hokey systems that is internal use only and requires human judgment and thought along with automation selectively applied; instead of a clear, clean, beautiful system built by hundreds for use by tens of thousands and costing many millions.

Conclusions

We are starting the part where we try to run through Molasses. But the visible hand of my HTML markup will start to add a few leaps and bounds and we will see where we are next week… The goal is Defined in 6 months – but we are still Initial at week 3...

[1] https://en.wikipedia.org/wiki/Turtles_all_the_way_down – a really interesting article on this...
[2] https://en.wikiquote.org/wiki/Helmuth_von_Moltke_the_Elder – more interesting stuff...