All.Net Analyst Report and Newsletter

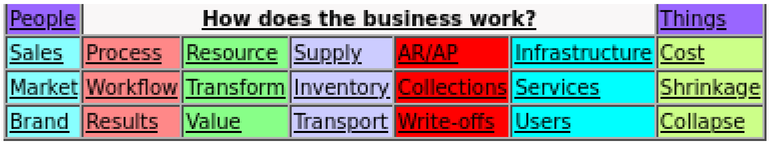
Welcome to our Analyst Report and Newsletter

The first steps in your cyber security program

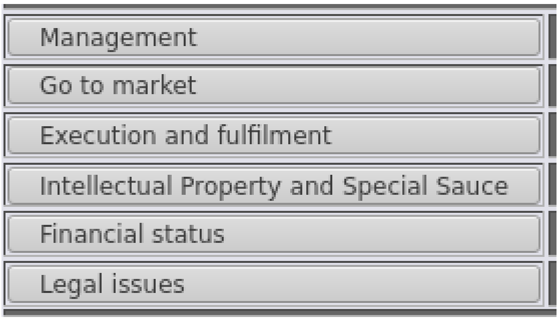
A fair number of folks have been asking lately about what the best first steps in small company cyber security program development look like (a.k.a., We're a small company… what should we do about it?). As I thought about it, the answer is pretty much the same as for a large enterprise, and the answer is not on the Top 10 lists you are likely to find in most forums.

Step 1: Understand your company

I've probably said this a hundred times (this month), but the first step for any company is to understand what makes the company work and what could make it fail. Ignore what you have done to mitigate risk, technology details, and pretty much everything else, and start with this list:



People	How does the business work?					Things
Sales	Process	Resource	Supply	AR/AP	Infrastructure	Cost
Market	Workflow	Transform	Inventory	Collections	Services	Shrinkage
Brand	Results	Value	Transport	Write-offs	Users	Collapse



Management

Go to market

Execution and fulfilment

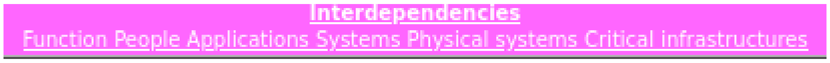
Intellectual Property and Special Sauce

Financial status

Legal issues

- What is how critical to success?
  - If you cannot manage effectively what happens?
  - If you are unable to sell, how long will you last?
  - If you can't execute on your promises and fulfill orders, what will happen?
  - If your intellectual property and special sauce lose their utility, what happens when?
  - If you cannot control the financial situation, when will the company crash?
  - At what point will the legal and regulatory environment destroy the company?

Step 2: Understand your dependencies on cybernetic systems



Interdependencies

Function People Applications Systems Physical systems Critical infrastructures

In the realm of cyber-security, we are predominantly concerned with cybernetic systems: sensors, actuators, communications, and control – including the people, things, and context they operate in. It does no good to have your people ready to work if they cannot get to the work to be done, and it does no good to have work to be done and no people able to do the work. If they are working from home during a pandemic and cannot get connectivity, they cannot work together or work with others.

- Business functions depend on people, applications, systems, physical systems, and critical infrastructures. Identify those dependencies and how they work.
  - It's pretty easy to test this. Turn things off and see what happens.
  - Do it during planed maintenance periods to avoid problems.

Step 3: Decide what to do about it

A business is a composite of its component parts. Faults in components lead to failures of the composite unless there is redundancy. There are two basic approaches:

- **Strategy 1: Fault avoidance (intolerance):**
  - Build a business (the composite) out of components (people, things, etc.) that don't break (i.e., fail to meet the business need) so that the composite does not break.
- **Strategy 2: Fault tolerance:**
  - Build a business assuming the component parts will fail so as that the composite succeeds even when (some of) the component parts fail.

Hint: Nothing lasts forever, so use strategy 2 EXCEPT when it costs too much:

- **Example:** Instead of one over-worked full-time person. hire 3 under-worked part-time people. If you grow, you can move them toward full time, each knowing how to do the others' jobs. If one becomes sick, you still have people to get the job done.
- **Example:** Instead of buying a single large printing press at one location, but 3 smaller ones at three different locations. But if this means 3 times the workers, perhaps it's too expensive...

How much redundancy is enough?

This is a tradeoff between risk and reward.

- For high consequences (business failure), make sure there is no single point of failure (SPOF), or if there is one, that you have a way to recover in time.
  - **Example:** Internet outage causing disruption of a major real-time quarterly event
    - Provide redundant Internet connectivity (~$100/mo), a redundant computer ($200 lasts for several years), a redundant person (more complicated…), etc.
  - **Example:** Internet outage causing some online meetings to go awry
    - Provide redundant Internet connectivity (~$100/mo), a redundant computer ($200 lasts for several years), but no redundant person.
  - **Example:** Internet outage causing one person low quality in meetings for a day
    - Apologize about the outage causing low quality and continue.

Match the surety with the consequences

Remember medium and low consequences become high if there are enough of them. Be careful of risk aggregation (the effect of many small cuts). Also remember that redundancy means **separate AND different**.

- Having two copies of the same book on the same shelf in a fire will likely wipe out both or none.
- If you keep them in different places (separate) and in different storage types (one in a fire safe, the other on the shelf), common mode failures are far less likely.
- If one copy is a digital one, a digital outage won't make the book unavailable.

Under what conditions are you willing to fail?

If there is an asteroid hit that kills 90% of the people on Earth do you want your company to survive it?

- What will it take to do that?
- Is it worth it?

For most companies, this potential event sequence is not worth worrying about.

- But for some nation states, and some individuals, it is worth the day-to-day price of trying to mitigate even this scenario.
  - **Don’t worry about things you don’t care about!**
    - But how do I know what I don’t care about?
      - **Ignorance is not bliss – it’s suicide.**
        - How do I make sure I’m knowledgeable enough to make good decisions?
          - **Like any other aspect of your company, apply expertise**
            - How do I get an expert? What will it cost? Etc.
              - **Like most things**
                - You pay for what you get
                  - **But you may not get what you pay for**
                - You will know if you want it by your willingness to pay
                  - **Is it worth it to you?**

Which of these things can I control?

You cannot control everything. Neither can I. But you can control some things. I generally start with the highest consequences and work my way down.

- If the cost is not worth the benefit in my mind, I don’t do it.
- If you live long enough, all of it will happen.
- We only know the frequency for frequent things.

Be aware that there are many ways to meet these challenges. Generically, you can avoid risks by not doing risky things or finding a less risky way to do them. You can transfer risk to others by contracts and insurance (read the policy carefully). You can mitigate the risk by taking countermeasures, like redundancy, better worker training, etc. And you can accept the risk and go on about your business.

Conclusions

This is not a top 10 list or anything like that. It’s a way of thinking about cyber-security (and running your company). Start with how your business works and what could go wrong, rank what could go wrong from worst case to best case, and find ways to make sure it goes right, unless it’s too expensive to be worth it. And if the consequence is high, and your solution is too expensive, seek another solution...