All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

I'm getting bored with the talk of the board

I was at a very nice meeting of CISO types yesterday, and they got around to the discussion of the way to communicate to the board of directors. Being the way I am, I could not keep myself from speaking up occasionally. Here are some of the things I thought they got wrong and right. Perhaps the most interesting thing was the discussion about...

What to tell the board

My view is that the first thing out of your mouth should be the most important summary information you can provide. Notionally, something like the following two sentences:

- The losses from cyber-related incidents was $XXX last quarter, while the expected loss was $YYY. The cost of the program was $ZZZ.
- We anticipate this quarter's expected loss in the range of $AAA to $BBB, while the cost of the program will be $CCC.

You should be ready to answer any questions. In particular about why these things are true.

I got some push back...

First off, that's a good thing. Fortunately, this was an opinionated, experienced, smart group of folks who are professionals at what they do. Several of the folks on the panel regularly report to their boards. Here is my minimal summary of what they said (and I said/say):

- You cannot codify this in money (then you should not be telling the board).
  - Of course you could also codify things in terms of the published mandates of the company – after you specify the financial implications in money terms.
- The expected loss is unknowable because … (you have to do better than that)
  - The future is always unknown, but that doesn't make it infeasible to reasonably anticipated. Sales projections are also unknowable, and yet we do projections.

A minor note here. The board should be concerned with material losses. See COSO.

Everything will change with the new regulations and fines

I wouldn't be so quick to judge this. The newest regulation to hit is the requirement for disclosing board membership expertise in cyber security. Here's what was expressed:

- There is a requirement to have a cyber security expert on the board (not true).
  - The actual regulation merely states that you have to list such expertise on your quarterly and annual reports. It says nothing about requiring such an expert.
- Companies without adequate expertise on the board will be shunned (wanna bet?)
  - They notioned that the reporting requirement would cause institutional investors to run away from companies with little, no, or inadequate expertise on the board. I expressed that we don't know what they might do, and they might just ignore it.

They talked about having a friend on the board

This is a great idea. I think they used a different word than friend – perhaps advocate is a better term. The point is that the CISO with a regular communication with a board member is much more likely to have the support they need and the board is much more likely to have good information that way. I think this is a great idea.

They talked about providing lots of details to the board to support the claims

My view is they get this stuff only if they ask… but you should be ready to provide it at all times… because you should know it at all times if you are the CISO. There are a few reasons for not spewing it out at them or handing them a 100 page document full of details. Such as:

- What you provide them, they may have a duty to read.
  - So you will not likely be invited back. You should provide the same level of depth associated with other reports provided to them. See how much information the CFO provides and try to match it in nature and detail.
- It may create liabilities – or they might think it does.
  - While I thing fiduciary duties require some level of depth of knowledge, the right depth is important to understand. The underlying question is one of priorities, and trying to force different priorities may harm the company. They take risks for rewards. They need to understand those risks.

We discussed the role of the audit committee

And the horror stories began. Did you know that the internal auditors don't always ask the right questions? Were you aware that they often just try to check the boxes on their requirements and don't have a clue about what they should ask? If that's true, its probably at least partly your fault. That's because you probably try to keep them as ignorant as possible because you want to pass the audits. And their job is to find things to report on (or not).

Suppose you told them that the questions they are asking are inadequate to what the board needs to know and provided them with a more complete picture? Maybe that would help inform the board and get the auditors on your side helping you to identify things you missed. … Probably not… but it may be worth a shot.

We talked very briefly about fiduciary duties

Very briefly of course. The underlying issue is one of reasonable and prudent decision-making. In other words, due diligence. They should be diligent and make reasonable and prudent decisions. Part of that process requires that a person with adequate expertise provide information to them and answer their questions, or that one of them has the expertise and takes proper care. Identify what they need to know to make good decisions and tell them.

As a hint, COSO[1] talks about things with a material effect on the company. How much is that? I imagine that unless it's at least a few percent of the gross sales of the company it will not meet the threshold. Or perhaps for companies with small margins and large gross sales it's missing the financial target the company otherwise would have easily made. Another hint, look up due diligence and reasonable and prudent in a legal dictionary.

1 The report of the Committee Of Sponsoring Organizations

Some call and response:

- The consequences of cyber attack might put the whole company out of business.
  - That should almost never be true for any reasonably anticipated event sequence, and certainly not for any single point of failure. Of course for a one-person company… and for a meteor strike killing everyone on the planet...
    - If I was on your board and you told me that, I would explain that this must change immediately. It represents a failure to address risk aggregation adequately. But a story may help…

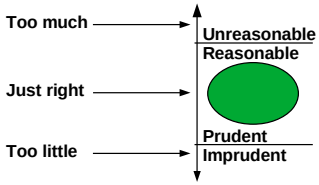
  A long time ago in a city far away, I did an assessment of the security posture of a large enterprise whose CIO had decided (no doubt under financial pressure to perform) to save money by consolidating data centers. The consolidated down to one data center.

  In my report I stated that this was too far and added some flavor by indicating that according to the media (history), one of their largest competitors had gone out of business only a few years ago when they did the same thing and had a major outage at their data center.

  The CIO called me into a meeting late in the evening to ask me to remove this from my draft report. They also told me that their director of IT had told them that this was considered "best practice" in the industry. I explained to the CIO that there was no such thing, and that if there were, this would not be it.

  I don't know if the director was fired, but the CIO was. My first recommendation on the first page of the report was that they immediately fix this problem (which they could do because the previous secondary was recoverable) because it could put them out of business as it had done to a competitor recently.

- It's "best practice".
  - No, it's not. Whenever I used to hear this term, I told people to stop it. Now days I explain that the better term to use would be "reasonable and prudent" practices.
    - But that also requires that you actually do what's reasonable and prudent (which by the way is also the way to not be negligent).



What is "reasonable and prudent"?

My quick version: (1) Situation-dependent, (2) Seriously considered, (3) By an expert, (4) In light of history. The CISO is supposed to be the expert doing this for cyber-seurity, perhaps getting the situation part from others in the enterprise, perhaps with outside advisors per many standards, etc.

Conclusions

Most of us hope and desire that "the board" will spring to life and understand how important the cybersecurity function is to the company. But few of us consider that they may actually know what they are doing when it comes to dealing with a CISO, or that the reason they do not is because the CISO doesn't know what they are doing when it comes to dealing with the board. Try putting yourself in their shoes and recognize that consequences drive decisions.

