All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

In anticipation of litigation

I keep reading about the health care massive cyber security failures, and the water systems... and power systems... cities... towns … you name it – all keep having cyber security failures.

But my experience is that, while they will pay for a quick fix that ultimately fails to save them from it happening again, they won't pay to find a sensible and predictable path forward.

How do I come to believe this?

Here are just a few examples from the last year to get you a sense of this:

- A major critical infrastructure provider for a nation state was successfully attacked. After a month or so of negotiations, they agreed to pay $25K for urgent assistance. Along the way we did a preliminary overarching review – just to figure out enough to understand how to start to actually solve their problems. It has been a year since then and they have not taken actions to mitigate any of the things we found or even to make a plan to go forward. How do I know they haven't done this with someone else? We know the top executives.
- A billion dollar facility looking to install a new multi-million dollar cyber security system expressed concern about having a cyber security review before connecting it to the rest of their environment. They had never looked at cyber security before. So they were offered a path forward with an initial study to determine what they currently had in place and how the new installation would effect the rest of their facility. No go. The initial claim? They didn't want to induce liability. I guess they would rather not know. They just want a price for a security system without having any sense of these issues.
- A company seeking to win a large part of the multi-trillion dollar a day international funds transfer arena and proposing a solution using blockchain technology was offered a free initial review of their cyber security posture as part of the due diligence for potential funding and to understand what they would have to do to meet the requirements of actual implementation. Sorry – they are not interested in knowing.
- A multi-billion dollar manufacturing enterprise was starting a cyber security program for their operational technology facilities. The program manager and their team of 3 had an annual budget of less than $50K. They were spending it this year on adding separation between the IT network and the OT network through identity management firewall pass-through. We managed to slip in an initial baseline and path forward at a slight loss to help them out.
- A large national power provider has a desire to understand cyber security issues, but the individual in charge has no budget for such a thing and cannot get one for at least another year – if then. They are using the slice and dice strategy of paying for it with multiple under-threshold purchases at a pace that will get it done in a year.

There are plenty more where that came from

At this point, I have to wonder what inside counsel is advising executive management in terms of cyber security. It can hardly be said that it's not important enough to worry about (under COSO[1] for example), given that:

- It's clearly material (consequences typically range well in excess of 5% of the total value of the company), and
- Many others (and likely they) have suffered significant publicly known incidents.

It's all over the media:

- Nation states and lots of others succeed in harming companies on an ongoing basis.
  - And that's just the things we read in the newspapers (or see on cable news {or find out about via the Internet [or learn via collaboration with our industry/other ISAO[2]]}).
- In January, 2020, the Department of Homeland Security (DHS) issued a National Terrorism Advisory System (NTAS) bulletin describing the threat posed by nation-state cyber warfare programs.
  - And then there are the election/registration system breakins and the explicit claim by one of the big voting machine vendors favoring Republicans (years back).

At some point, you have to hit the negligence level by continuing to ignore the reality around you and failing to even seek to understand the issues within your company. And yet there remains strong resistance to finding a path forward for cyber security programs using independent experts.

- Independent: Don't care about internal politics, just want to get to the truth via facts.
- Experts: Knowledge, skills, education, training, and experience in relevant matters.

But I don't want to!

I imagine all sorts of reasons for these sorts of decisions and inaction. But really, most of the reasons I likely hear are the justification for not doing something that they don't want to do for some other reason. They may not even know the actual reason. So if you are a corporate counsel and you work for a company that has not identified what they do in terms of cyber security or the plan going forward, I think it's time for you to make them…

An offer they cannot refuse

The offer is this. Corporate counsel will engage outside counsel to review the current state of cyber security and a potential path forward, and over time, will work with management and executives to address these issues, **in anticipation of litigation**.

Yes, that's right. Because of the lack of understanding of cyber security within your company, you are subject to potentially unlimited liability, and legal counsel anticipates that litigation may result. As such, top management should reasonably decide to find out the real nature of the situation and how/if it should be addressed.

---

1 Committee of Sponsoring Organizations of the Treadway Commission, which is cited in regulations as a basis to put executives in jail if they fail to follow the framework or do something equivalent.

2 Information Sharing and Analysis Organizations have been in place for over 10 years now.

How is this better than other approaches?

Working these issues through counsel until you become comfortable doing it directly, has several advantages, and it is a proper thing for counsel to suggest:

- It is in fact in anticipation of potential future (or currently pending) litigation if your company has not yet come to understand these issues otherwise, because litigation is now common in cyber-security-related matters and you should be anticipating it.
- In anticipation of litigation, legal counsel may act on behalf of client under attorney client privilege, including through the use of experts. This often eliminates concerns about inducing liability by knowing of the situation, because the privilege can prevent those involved from answering questions about what was discussed with counsel.
- Having outside counsel engage experts to help understand these issues means that anyone claiming negligence in this regard would have to show that this is not a reasonable and prudent approach. Having well qualified experts review things is, in may ways, the heart of being diligent. Intentional ignorance may be the opposite.
- In order to prove anything about details, the other side would have to penetrate attorney client privilege, which is very hard indeed. Of course this doesn't prevent someone from finding out what your company does through legal means, but how the decisions were made may become protected in a different way through counsel.
- If done properly, unlike an audit or other sort of assessment, this process will not create internal frictions or refusals to participate, except possibly by workers who are intentionally acting against the well-being of the company. In my experience, having the legal department involved carries a higher level of seriousness and cooperation.
- From an investigative point of view, as/if something is encountered that is problematic and calls for an investigation, it will be important for legal counsel to be involved. Sadly, we sometimes encounter such a need even when not looking for it.

Why outside counsel?

In most cases I have seen, inside counsel has plenty of work to do and lacks the specialized expertise for issues surrounding cyber security. This area calls for specialists. However, it is important for inside counsel to get involved in the process, and over time, to stay involved in understanding these issues and advising top management and the board.

Not my first rodeo

This is not a new idea I just came up with. I have worked on matters for outside (and in house) counsel before, and these very sorts of things were done for these very reasons. In some cases, it also makes things a lot less disruptive to the company when/if litigation appears. It limits the need to get employees involved and reduces the chances that they will communicate things in ways that, while honest, are not necessarily optimal for legal purposes.

Conclusions

Litigation will come and ignorance is not bliss. Willful ignorance is, perhaps negligent, and certainly not a sound approach. Gaining clarity around how cyber security will enable your path forward and enhance your success is certainly reasonable and prudent. The legal department as a path forward can mitigate fears of inducing liability by finding out.

