All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

CISO jail time (not really, but...)

Do you want to be fired or do you want to go to jail? (hyperbole: in a civil matter it's not jail)

OK, very few CISOs have ended up in jail, and none so far for merely under-reporting of material weaknesses. You have to go all the way to fraud. And fraud means, in essence, theft by deception.[1] Of course we are talking about the Security and Exchange Commission charging the Solar Winds CISO with fraud.[2] The actual complaint[3] asserts that:

> *"Defendants SolarWinds and its then-Vice President of Security and Architecture, Brown, defrauded SolarWinds' investors and customers through misstatements, omissions, and schemes that concealed both the Company's poor cybersecurity practices and its heightened— and increasing—cybersecurity risks. SolarWinds' public statements about its cybersecurity practices and risks painted a starkly different picture from internal discussions and assessments about the Company's cybersecurity policy violations, vulnerabilities, and cyberattacks."*

To be clear, I don't know the facts of this case. All I know is what is alleged and what has been in the media.

The alleged facts

I really like the way most of the federal complaints I have read present information. It's easy to read and to the point. Here's what their CISO said in their SEC filing, per the complaint:

> *"current state of security leaves us in a very vulnerable state for our critical assets"*

Now when I wrote things like that in reports, I was always told by my customers that they didn't want that in the report, and I explained to them that the reality is the reality. Perhaps it was a bit understated, but hardly a lie. Here's an example of a finding from one of our reports (details redacted of course):

> Key finding 1:
>
> Single points of ***-wide failure are being introduced or worsened through this effort leading to increased chances of *** collapse
>
> The new data center is being made a single point of failure, is in a flood plane, is off the end of an airport runway, and locates critical resources on exterior walls
>
> There is a single key individual who is not cooperative, is behaving like a disgruntled employee, and who is in sole control over the most critical elements of the effort
>
> The single perimeter approach is eliminating necessary redundancy that provides for continuity of services and *** continuity
>
> Project efforts should halt until these issues are addressed

Of course what we got was fired… after we refused the bribe attempt. They got jail time.

1 Fraud is defined as *"knowing misrepresentation of the truth or concealment of a material fact to induce another to act* to his or her detriment" – Black's Law Dictionary
2 https://www.sec.gov/news/press-release/2023-227
3 https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-227.pdf

What do you expect?

The underlying problem is and has long been fundamental to the cybersecurity profession at high levels within enterprises of all sorts. Top management really wants good news. And if you tell the truth in a direct manner, you will get fired.

But apparently, the SEC is telling the CISO that if they aren't fired, they will be prosecuted.

Now as I said, I don't know the details of this case and the facts available to me are limited.

Another example?

I have had similar results from consulting gigs more times than I can remember. To find that example from my archives I ended up looking through a few score and recalling some of the more interesting details long forgotten. A fired CIO who asked that we soften our report. A VP who refused to pay us until we changed the report, until we pointed out a contract term that was sufficiently onerous. The list goes on and on.

How do you get out of it?

We always just told it like we saw it and backed it up with facts. But then as a consulting group, we didn't have the same internal forces aligned against us. And our contracts always stated that we were not liable for anything. And… and… and...

Work with good people

But the real thing to know is that the vast majority of our clients over the years called us in to find out what the did not yet know. And that is really the key to keeping your job and telling the truth. If you are underpaid, or undervalued, or underfunded, or otherwise having problems in your job, it is likely because the people you are working for don't respect you. If they don't respect you, you should not be working for them… assuming you deserve that respect.

Be reasonably polite – but direct

Which brings us to part 2… you need to know your job, do your job, and not worry about losing your job. I have a saying: You cannot do your job if you're worried about losing your job." Knowing your job means studying your profession, keeping up to date, getting outside assistance when reasonable to do so, and for the most part, being a professional. There are codes of ethics that you should follow, and we follow the IEEE Code of Ethics and the $(ISC)^2$ Code of Ethics. We don't just say we do it, we actually do it, as well as we can.

However, to say that the regulatory guidance is unclear would be a gross understatement. There are obvious problems with releasing too many details of internal issues, because this information can be exploited by threat actors, not only directly by the focus of attention on specific lines of attack, but also indirectly by allowing influence operations to focus on specific things known to be potential problems.

And to be crystal clear, the same standards should likely be applied to financial information. For example, Coca Cola knew of the value of its trade secrets and didn't warn the SEC that someone could take them, especially if an insider was involved. And Target knew it has external companies with access to its network that could potentially be used to exploit their content and mechanisms for any number of things, only one of which was an information leak. Should Target have disclosed the other things that might have been done with that access?

Some examples from SolarWinds

According to the complaint:

> *"The Security Statement was materially misleading because it touted the Company's supposedly strong cybersecurity practices. For example, that statement asserted that SolarWinds created its software products in a "secure development lifecycle [that] follows standard security practices including vulnerability testing, regression testing, penetration testing, and product security assessments." And the Security Statement claimed that SolarWinds' "password policy covers all applicable information systems, applications, and databases [and we] enforce the use of complex passwords." It also stated that SolarWinds had "[a]ccess controls to sensitive data in our databases, systems, and environments [that are] set on a need-to know / least privilege necessary basis." All those statements were materially false and misleading."*

But is it the lack of honesty on the part of SolarWinds or a lack of comprehension on behalf of the government? Here is how I interpret these things:

- a "secure development lifecycle [that] follows standard security practices including vulnerability testing, regression testing, penetration testing, and product security assessments."
  - Which standards precisely are they using? Vulnerability testing does not imply finding all or even most vulnerabilities. Regression testing means looking for the things you previously found to make sure they do not return. Penetration testing means someone else was paid to try to break in. Product security assessments means that someone looked to see what they could find and reported it.
    - The government asserts that "*(a) failure to consistently maintain a secure development lifecycle for software it developed and provided to thousands of customers,*", but the assertion above is that the software was created with such a cycle, not necessarily maintained with one.
- "password policy covers all applicable information systems, applications, and databases [and we] enforce the use of complex passwords."
    - The government asserts that "*(b) failure to enforce the use of strong passwords on all systems,*" but the claim as asserted was not that this is in place for all systems, only all "applicable" ones, whichever ones those might have been designated as.
- "[a]ccess controls to sensitive data in our databases, systems, and environments [that are] set on a need-to know / least privilege necessary basis."
    - The government asserts that "*(c) failure to remedy access control problems that persisted for years.*" but again, this is not contrary to what was stated.

Again, I know none of the facts here, but as someone with expertise in the area, I don't take such statements at face value, and neither should investors. No more than any other statement in company filings. I am willing to bet that if you look at every public company, you will find all sorts of similar things.

How sophisticated are investors?

Generally, the answer is, not very. In order to make it clear, I think every company should state, with very few exceptions, something like this:

> We use cybernetic systems and technologies that are inherently problematic, as does every other company we are aware of. These technologies have historically shown a lack of integrity, availability, accountability, use control, transparency, and confidentiality. They operate on hardware and software created, in many cases, by people and companies from nation states that are known to place malicious capabilities within them intended for exploitation, and these mechanisms are commonly exploited for these purposes. Our company can, at any time, be compromised in material ways resulting in large-scale loss of investor value, just as every other company in the World that depends on cybernetic systems for success. In addition, our company depends on other infrastructures providing physical, cybernetic, and human resources, owned and operated by other companies, any and all of which are almost certainly subject to the same issues, and issues affecting those companies may also effect ours. The number of specific things that can go wrong are unlimited, and nobody is able to identify all of the possibilities going forward. Threat actors of all sorts attempt to bypass our controls many times each second, and we would go out of business if we spent all of our resources trying to eliminate every single one of them. There are most certainly many vulnerabilities in our systems we are not yet aware of, and more that will be discovered over time.
>
> We have limited funding and support for internal programs to mitigate the potential bad things that can happen, we use insurance to transfer some of the potential negative consequences that could occur, and our top executives choose to accept risks as a normal part of their efforts to move the company forward. When we encounter problems, we seek to prioritize their mitigation in the context of the overall business, and that means not fixing everything we find as soon as we find it. We seek to balance the costs with the potential consequences, through our risk management program, which is managed by our risk management team under the direction of our Chief Risk Officer under the supervision of the CEO and as reported to our board of directors.

As you read through the filings I reference, I think it would be a really good idea to understand the difference between what the average person on the street understands about these issues and what professionals understand about them.

Conclusions

I don’t know the facts behind the SolarWinds case, and there may be intentional deception for financial advantage involved, the CISO may be responsible for it or not, and that is not my point. My point is that the risks are there for all of us, every day, and if you don’t understand this, you should. To the extent that the average investor is unaware of these things, it should be made clear to them. It should be clear to all of us, and it now is... because you got to here.

However, it is also important to add, that the introduction of cybernetic systems into the world has, over time, brought about tremendous improvements in human life. Along with the potential problems come the already realized benefits. This, however, apparently does not belong in such government filings.

