Schulte Roth&Zabel

New York | Washington DC | London | www.srz.com

HFMTECHNOLOGY

Q&A

LEGAL DEFENCES

As cyber-security continues to remain a key focus for hedge funds, there is a growing number of questions surrounding the associated legal issues and requirements. *HFMTechnology* speaks with three leading attorneys at law firm Schulte Roth & Zabel about some of the challenges facing firms and how managers can mitigate any legal risks emerging from cyber-security.

MARC E. ELOVITZ
Partner and Chair of the Investment Management Regulatory & Compliance Group

HFMTechnology (HFMT): What is your view of regulators' approach to cyber-security in the industry?

Marc Elovitz (ME): From the SEC perspective, the focus has been really a matter of scoping and trying to figure out what are the actual risks that hedge fund managers face and to see what incidents firms have had. For every hedge fund manager they need to think about it in terms of – did I do something wrong or am I going to be the case study the SEC trots out?

While the SEC is in the process of gathering information to inform its regulation going forward, it is not precluded from bringing enforcement action and charging individual fund managers.

Brian Daly (BD): I think the SEC would say they have a fairly robust and specific set of rulemaking guidelines out there and what our fund managers are worried about is who will be the first hedge fund prosecution. It is true that there is no cyber-security rule per se but if you look at the releases that have come out there has been a lot of activity and there has also been an extension of Regulation S-ID which now includes hedge fund managers and commodity pool operators. Virtually all of the entities registered with the SEC and CFTC are covered by it.

In addition, hedge fund managers and commodity

pool operators need to have business continuity/disaster recovery policies in place.

Michael Yaeger (MY): They are putting a lot of time into this at OCIE and the different US Attorneys' Offices are making cyber-security a focus too.

There are specialised units developing in different prosecutors' offices for this. My old office, the US Attorney's Office in Brooklyn, has a cyber-crime unit and I know that New Jersey is certainly making a big push into the area, and Cyrus Vance in New York is doing the same.

Furthermore, many states in the US have breach notification laws. They mainly concern personally identifiable information – mostly of investors – but it could also be that a particular fund has an investment portfolio where they have certain kinds of data and if that information leaked they would have a breach notification law.

So aside from the SEC, there are several other regulators which firms need to be aware of and ensure they have the relevant controls in place.

BRIAN T. DALY
Partner, Investment Management Regulatory & Compliance Group

HFMT: How are you assisting fund managers with cyber-security issues?

ME: A very common area stems from phishing attacks. Some of the defences are clearly just training staff to recognise rogue emails but there are additional add-ons like managing your IP rights that you can put in place.

If you do find someone creating an account or web address similar to your own you can actually go after them and that domain name and try and get possession of that. We have done that for clients in the past and while there are filters and training, there is legal assistance that can help.

We also work with a whole range of hedge fund managers on their policies and procedures across the board so when it comes to information security issues there is a real hunger among managers to have polices in place.

Firms can be very different in terms of IT architecture and risk, and each firm should really have a tailored policy that reflects what its make-up is like and what it is doing to protect them.

MY: We have been seeing an interesting mix of compliance-centred questions and also reaction to particular events.

First of all people are coming to us to develop their cyber-security readiness plans, which of course involve having an incident response plan but in addition firms are also coming to us because they want to have contracts with their vendors that protect against outside risks. And some have come to us to handle particular incidents, such as attempted intrusions and insider-incidents.

HFMT: How important is it that firms have strong contracts agreed with third-party vendors?

BD: One thing we see a lot of our clients doing is going to third-party vendors to check up on their other vendors and internal policies.

This is an industry which is very quick to coalesce around 'best of breed' vendors; however, we caution our clients to vary their service providers and not to have the same consultant come and do the same analysis; because if everyone relies on the same testing and the same vendor, it introduces a new kind of systemic risk to the industry.

Firms should also identify any sub-contractors that have access to information and provide due diligence material for those firms. The chain goes several steps back and you want to know where your data sits.

MY: There are a lot of third parties that touch the systems of a hedge fund and so that is a natural vulnerability.

We want people talking to their vendors about what they are doing to protect their security. The mere fact your data sits off-site doesn't mean you don't have an obligation for it. You need to know what vendors are putting in place and how they are going to notify you if something happens and funds have notification obligations as well even if a breach occurs off-site.

It also make sense to interview several vendors before you hire one and there is always something to be learned by having several people answer the same questions.

HFMT: Have you seen an increase in firms requesting dedicated information security policies?

BD: We definitely see more interest. Managers are asking a lot of the right questions and starting to grapple with it. There isn't yet a clear and universal standard but there are emerging rules.

Cyber-security in some sense is just the digitalisation of all risks you already had. Some of this is managed through HR policies – for example information security, appropriate use, and BYOD policies – and that means those policies need to be re-written to cater to cyber issues and we have been re-writing certain policies for people.

MICHAEL L. YAEGER
Litigation Special Counsel

ME: There is so much data at a hedge fund manager that it is accessible to the employees that is at risk because of the potential for rogue employees but more frequently just the employee who doesn't take enough care.

The most important thing is doing the work to make sure you are protecting the information. But your approach also should be embodied in a policy that is tailored to your business and your risks, that provides notice to employees and that shows the regulators the approach you are taking.

HFMT: How prepared do you think the industry now is to possible cyber-attacks?

ME: I think awareness is at a much higher point now. It can be a scary topic but in another way it should be re-assuring – this is risk management. This is not supposed to be something totally foreign to the operations and technology departments. It is all about understanding your business model and how technology affects that model.

> "Cyber-security in some sense is just the digitalisation of all risks you already had. Some of this is managed through HR policies... and that means those policies need to be re-written to cater to cyber issues"
>
> Brian T. Daly

MY: There is a whole class of criminal who are not very technically sophisticated and buy crime-ware. A criminal goes out and buys some malware and then has a dashboard which he can use to monitor his access points into different systems. Some of these guys don't have much technical knowledge but they are able to use the purchased malware and if a company isn't doing basic things like patching its software for known vulnerabilities, this commercially available crime-ware can exploit it.

While people are definitely making greater strides to address the area, I do think there is a tension in cyber-security. On the one hand there are these super-sophisticated hackers at the top end but an enormous number of firms won't ever actually face those threats; on the other hand, people aren't always protecting themselves against more simple attacks, and failing to do that increases compliance risks.

There is no such thing as perfect security but ultimately there is a limit to the number of places those sophisticated actors are going to be interested in, and taking reasonable security measures can reduce your risks. ■