Proactively Addressing Hedge Fund Cybersecurity Risks

Q&A with Marc E. Elovitz and Michael L. Yaeger, SRZ

IN CONVERSATION WITH ROD SPARKS

The Hedge Fund Journal spoke to Marc E. Elovitz and Michael L. Yaeger of law firm Schulte Roth & Zabel LLP about the growing need for cybersecurity policies for hedge funds, both in light of recent regulatory attention and the increasingly prominent attacks on major corporations.

Marc E. Elovitz, a partner in the New York office of Schulte Roth & Zabel LLP, is chair of the firm's Investment Management Regulatory & Compliance Group. He advises hedge funds, private equity funds and funds of funds on compliance with the Investment Advisers Act of 1940 and other federal, state and self-regulatory organisation requirements, including establishing compliance programmes, registering with the SEC and handling SEC examinations.

Michael L. Yaeger is a litigation special counsel in the New York office, where his practice focuses on white-collar criminal defense and investigations, securities enforcement, internal investigations, accounting fraud, cybercrime and data security matters, as well as related civil litigation. He spent six years serving in the US Attorney's Office for the Eastern District of New York, where he investigated and prosecuted cases in the Business and Securities Fraud Section of the Criminal Division. He also served as the office's co-coordinator for Computer Hacking and Intellectual Property crimes.

Rod Sparks: Why is cybersecurity for hedge funds coming under increased scrutiny?

Marc Elovitz: The SEC had a roundtable last March, the overall SEC, the whole agency, about cybersecurity risk and information security risks. It was a real wake-up call which followed a bunch of the large commercial companies, like Target, having incidents, and a realisation that the entity of the SEC itself and the entities that are regulated by the SEC face similar risks.

Of course since March, and since a year ago, this has only become more apparent, with Sony and these other big hacking incidents. They had that roundtable and what came out of that was the examination group that reviews hedge funds did what they call a "sweep exam" where they go out and they look at a smattering of different investment advisors – they also looked at broker-dealers – to see what they're doing in this area, and really gather information.

There are no specific standards that apply, there are no rules that apply to hedge funds to say this is what you have to do and this is what you should be doing, so it's really just a matter of the hedge funds' general fiduciary duties to their investors, and how you're protecting your investors and the steps that you're taking on that. Out of that sweep examination came the Examinations Group Risk Alert, which at the end of the day really gives very little prescriptive assistance in terms of what a hedge fund manager should do.

It identifies some of the risks and the basic frameworks, but there are huge question marks as to really in practice what needs to be done. I think at this point we've identified some of the general risks and how you might think about them, but the regulators haven't provided (and I don't think any time soon they're going to be in a position to provide) really specific information as to what should be done, which is why it's so important that the hedge fund managers do not sit back and wait for the SEC to say, "Okay, here's the very specific list of steps you are to take," but instead to take it on themselves.

And Michael has really become an expert in working with hedge fund managers about what they need to be doing right now in anticipation of not just further hacking incidents, but in anticipation of further regulatory scrutiny.

Michael Yaeger: The regulatory background here is in part from the Gramm-Leach-Bliley Act, and one piece of that is Regulation S-P and the need to have a written information security programme – and, that's not much more specific than have a plan! They don't give you an enormous amount of detail on what kind of plan you should have, but have a plan, and take reasonable security measures.

And this is mirrored in the state laws across 47 states and various territories like the District of Columbia, which has their own breach notification laws associated with investors, or customers. It all comes down to taking reasonable security measures; it's a very lawyerly sort of answer; what the heck is reasonable? And so what's happening is, there are emerging best practices and people are having to embrace that and talk to each other, follow various frameworks like the National Institute of Standards and Technologies Framework – a list of standards – so that they have a basis for the reasonableness of their actions.

Obviously, it's a little bit of a moving target, which is another reason why people have to be proactive on this. It is not synonymous, however, with "have absolutely bleeding edge security." Reasonable does not mean you have to have the best engineers at Google residing inside your hedge fund, but there is some uncertainty on exactly what's required. There are certain state laws, like in Massachusetts, that get very prescriptive: you must encrypt, you must have a firewall, various particular provisions.

But most of these laws speak in large terms of general reasonableness and duties, things of that sort. So there is a lot to be gained by doing risk assessments and understanding the particular problems you might have, given your business model: if, for example, you are a quantitative fund and you have very valuable IP associated with your trading strategies, those are things you need to protect more.

You have to do an assessment of what you have that is valuable, where it resides, and how it might be endangered. Where it resides includes all of your systems, but also all these mobile devices to the extent that certain information is out there, because it is no longer a purchasing department-driven world. There is the consumerisation of IT, and so a lot of purchasing decisions are driven by individual people because of the rise of the bring–your-own-device movement.

RS: What are you seeing from the investor perspective? When it comes to due diligence questionnaires, have you had experience of investors asking managers or putting managers to strict proof on their cybersecurity procedures?

ME: Yes we definitely have seen a ramping up of investor due diligence questionnaires and information requests related to cybersecurity. They have run the gamut really. There's no one standard set of requests out there; they vary. Some of them were focused on the issues specified in the SEC Review, asking, what are you doing to inventory your devices and your sources of leakage? Are you using any of these frameworks? Things like that.

Others have looked at it more from the perspective that investors often look at it as, "Who at the hedge fund is responsible for this and do they have the expertise for it?" and "Are you leveraging outside resources in an appropriate way?" Many hedge funds at this point are using not only internal resources but outside resources for some of the forensic reviews, and the investors like to see that.

They like to see that you're doing penetration tests and that you're looking to see how your systems hold up, and some of the more sophisticated investors are absolutely pushing for that type of work to be done affirmatively, as opposed to sitting back and saying, "Well, we think we're okay."

RS: Why is it important to address company policies and procedures even before regulators implement restrictions?

MY: Just to take one small example: it may not be the most important thing but it leaps immediately to mind, which is a programme of policies associated with a bring your own device programme. A lot of people are allowing their employees to purchase their own personal devices and have company information on those devices in addition to personal information. It raises a certain set of issues, especially upon termination: what happens to the company data and, if there are internal investigations which have to be conducted, how are they conducted?

When a company owns a device or system, it has more legal rights over that device or system than it does in the other situation. And what it needs to do is obtain consent up-front and to give notice to employees about the company's right, the firm's right, to wipe the firm's information and to image the device as a whole, if need be, in connection with an investigation. So it's not that these things are especially onerous or especially broad, but there's a clear need to give people notice before the problem occurs, and to review your policies to make sure that they're in line with your current IT practices.

If you have a BlackBerry-era policy in an iPhone age, that could be a problem. If you have a policy designed for procurement departments and not for individual personal purchasing decisions, that could be a problem. So things of that nature pose one example.

RS: Why are employee training programmes of particular importance?

MY: In particular what we worry about is so-called "spear phishing". A phishing scam is the old classic spam attack where people pretend to be a prince in a foreign country and they're down on their luck and there you are. They're kind of funny and ridiculous and easy to recognise, and a lot of them are caught in spam filters anyway. The spear phishing is more targeted, as the name implies. It is an attack designed for a particular company.

There's a lot of information out there, publically available for con artists – and that's what these spear-phishers are – to use. They can go on LinkedIn and determine a lot of someone's organisational chart, just by going on LinkedIn. And so then they can say, "Ah, this guy is in the treasury department and reports to this higher-up, I'm going to pretend to be his higher-up in this email, to spoof the email address of the higher-up and I'm going to ask him to send money out to this particular vendor." And so it's an email that looks like it's coming from your boss, not a Nigerian prince.

There is an attack of that nature, so it's becoming a little bit sensitive to this. We have seen these various sorts of attempts to get people to wire money out and they don't look as cartoonish as they would otherwise.

So training employees to recognise differences in their standard procedures, to slow down at those decision points—such as when someone is asking for money or log-on credentials, showing them samples of this, it's a useful thing to remind people. Some of it seems like common sense, but it's not so easy, especially if you're on a mobile device and you're in a very fast-paced, demanding environment and you're trying to respond to people quickly.

ME: And you think about the way a lot of hedge funds operate, which is that there is a premium on speed, being nimble, with people travelling round the world, and not having the type of corporate infrastructure where everything has to be signed and checked by 20 people before any wire is sent out.

There are typically procedures in place, but some of these spear phishing attacks, as Michael is saying, are pretty sophisticated. It really requires some degree of sensitivity to the issue and the last thing you want to be is the hedge fund that mistakenly sent the money where it didn't belong because you weren't thinking about this.

MY: Also spear phishing is a way that people can infect systems. The easiest way to get into

a firm's systems is to have someone execute a command. They're clicking on something and they don't realise they're installing software that they shouldn't on their computer. There are various technical protections against this, spam filters, frankly just limiting people's privileges so that if you were to hack my account it wouldn't be as valuable to you because I don't have the same level of access to the system as my IT guys.

There is a certain vigilance when people change roles within a company. They shouldn't simply have all their old privileges plus whatever new ones they need; there should be some thought to, again, what does he actually need? Can I restrict some of these other privileges? In that way, certain measures can help protect you from both outside and insider threats – that's one thing we haven't talked about as much: there still is a great deal of risk from the well-placed insider, because they're inside the circle of trust.

RS: In a recent SRZ cybersecurity update it says, "less than a third of the examined investment advisors surveyed have actually appointed" a chief information security officer. Did it surprise you to discover such a low take-up?

ME: No, well one thing to keep in mind on this is that if you frame the question that way, then you might get that answer – especially in hedge funds where there's not a typical naming convention. People have all sorts of different titles, so even at a firm where there may be a very sophisticated chief technology officer who is very sophisticated in information security, they might have answered no to that question.

So it doesn't mean that the firm doesn't have the personnel and hasn't put the resources into technology, information security; it just may mean a titling issue. And so I don't think you want to draw a negative inference from that. And the way that I think the regulators would actually look at it on a case-by-case basis is, who do you actually have doing this stuff internally? Do you have sophisticated people who understand what they're doing and are keeping up on things and have the resources to keep up on things and are utilising outside resources?

This stuff is moving so quickly now that no one person can know everything that's going on in the area. And so you can't hire that one person who's going to do it all for you; that person will necessarily, as Michael was suggesting, be part of these networks where they're talking to other folks, they're involved in them, and they're oftentimes using outside consultants to do the testing, to do that type of work in addition to what they might do internally.

MY: I think I would want to focus on the function rather than on the title. The issue there, and I think it's a question that if framed differently would have had a different response, would be "Do you have an employee who is charged with responsibility for IT security as distinct from operations?" Maybe it's the same person, but if there was an identifiable person who is in charge of IT security, taking that upon him or herself, now that, as Marc is pointing out, is also a coordinating role. Much in the way that your inside counsel procures outside legal services, your inside security officer can be purchasing outside services too.

It is the person who is your guide to this category of risk. So I certainly think that it is advisable to have clear lines of responsibility and someone who knows that this is his or her job, and it is a person who should not be so overburdened with other responsibilities that they cannot properly attend to security concerns – that they're so overwhelmed with operations that they can't think of that. But the formal title itself on the org chart is far less important than knowing who's your man or woman on the spot.

RS: When hedge funds are looking to implement a breach response plan, what areas should this cover, and how detailed should they be?

MY: One of the things that needs to be in place is a cast of characters, the list of people who are on your team. It is a multi-disciplinary response that should involve IT security (of course), legal, PR, operations. And this is, in many ways, an understanding that this is an exercise in risk management which, of course, funds are very familiar with. It's just how technology intersects with the kinds of risks they've always had, and being ready to handle things when they haven't been familiar with the regulatory requirements and the regulators they are subject to.

For example, where are your investors located? So what state laws might come into play? And being aware of the kinds of risks and how they would respond to these risks.

Some of this is, at a minimum, being ready for the low-hanging fruit. What happens if you have a lost laptop? What happens if someone has lost their phone? Not just the more exotic problems of a nation state hacking your order management systems or something – being ready for the obvious things, if nothing else, and having a plan in place. Having an idea of who you will turn to, having a disaster recovery plan in place. Some of this is also the technology risk; it doesn't always have to be some malicious attacker. It is simply a systems failure that could be disastrous.

RS: And are you aware of there being much co-operation or dialogue between firms? Is there a pooling and sharing of knowledge between chief technology officers and compliance people?

ME: There certainly is, and this happens any time you have an area where the regulation hasn't caught up with the risks and people are very eager to find out what the best practices are and what works and what doesn't work. So those kinds of dialogue, that's very useful in this as in other areas for hedge fund managers where there's not a lot of detailed guidance out there.

But the one peculiar risk here is that a lot of hedge fund managers are keen to avoid a situation where there's a herd mentality and a "group think" mentality where everyone is saying, okay, this is the risk, this is what we're doing and we're all doing this. And while it's good to get comfort from others and to know what they're doing, if there's this kind of herd or pack mentality it can mean that you're not really thinking about what your particular individual risks are as a firm – they may be missing that – but you also may get to the point where the testing that you're doing, the way you're analysing and looking at things,

everyone is doing things to the lowest common denominator. You're not really doing what you particularly need to be doing.

MY: So, for example, firms with offices in different cities, in different countries, have different issues. Firms with bring-your-own-device policies have different issues than firms that don't. Firms using different vendors with different systems that access info have different issues.

Different types of investments can also be relevant here. I mean what if you have as part of your portfolio certain kinds of loans with personal information? Then you're going to have to protect that and perhaps employ encryption more than some other firms might. Encryption can be valuable in terms of regulatory reasons, not just risk. There are many states that do not require you to notify people of a breach if the information that is accessed was encrypted.

On the other hand, encryption slows things down, it's inconvenient, so it's not simply that you're going to encrypt absolutely every single thing on your system. Depending on what your risks are you may encrypt more or less. And so some kind of rote idea of "This is what all hedge funds do so we're going to do it" would be a problem in that particular situation.

There's really no substitute for thinking about your own particular organisation. That said, people are very wisely talking to each other about what vendors they use and what kinds of things they ask their vendors to do.

RS: Michael, in your former job, did you come across many instances of the sort of breaches of security that we are alluding to in this conversation?

MY: Well, I certainly saw major corporations hacked, and there were a few situations where we in the government knew it before the organisation. I remember one distinct meeting where I had to sit there convincing the security officer and the executives that they had been hacked and, in fact, people had been in their systems quite a while. So that does happen. There are ways in which funds are not as big targets as large commercial companies. We don't have to pretend that every company in the world is exactly the same, that they face the same risks. There is a certain, I wouldn't say predictability, but there are sort of averages and general rules of thumb that people who are more forward in the public eye and have a larger attack surface have to worry a little bit more. It's not as if most of the hedge funds have a point-of-sale computer in the way Target and Home Depot do.

But there is no doubt that this is an area where the Secret Service and the FBI may know something before you do, which raises other sorts of issues of needing to coordinate the law enforcement when they contact you with how you do that. I mean that is certainly a situation where people would be well advised to talk to outside counsel who are familiar with this, may be familiar with particular regulators, and be able to interact with them.

Once the government's involved, to a certain extent, especially if it's a criminal investigation, the organisation has less control over the matter. Having lines of communication open can be helpful. But as we've seen, this is a really big deal. I think the public has expectations that organisations will work with law enforcement to try to solve the problem. This is a situation where, often, funds are victims. This is not always the same as other kinds of regulatory situations where there's a perception that the people in the financial industry are causing the problem.

ME: Though at the same time, from the investor perspective, they're looking at it, "Okay, it's our money that you're managing, even if you may be called the victim, you need to be protecting us, what are you doing to protect us?" And that's where you go back to the investor issues. **THFJ**