return to Cybersecurity Update

SEC could start issuing more exam fines for poor cybersecurity controls

Tue, 13/10/2015 - 09:41

The saying goes that 'familiarity breeds contempt' but when it comes to staying cyber secure, nothing could be further from the truth. Fact is, investment managers should be integrating cybersecurity issues, be they regulatory updates, software updates from their IT vendors, into their weekly meetings.

Even if it takes up just a few minutes of the agenda, getting into the habit of keeping staff aware of cybersecurity developments will allow it to become part of a firm's broader risk management program and potentially mitigate human error; often the cause of so many internal data breaches.

In other words, cybersecurity should be part of an ongoing risk assessment, not something that gets reviewed once a year.

"As part of our ongoing compliance and regulatory support for firms, we certainly hit on cybersecurity in just about every training session that we have but we also encourage them to have those conversations internally to reinforce the message," says Buddy Doyle (pictured), Founding Principal, CEO & Managing Director of Oyster Consulting, a leading advisory firm to the investment industry. "We also advise our clients to have a cyber risk policy in place as part of their overall insurance plan because it can potentially be very expensive if they incur a data breach."

Indeed, one only has to refer to the recent case on 22nd September 2015, when the SEC charged a St Louis-based investment adviser for failing to have proper cybersecurity measures in place to appreciate the extent to which regulators are focusing on cyber crime. The firm in question, R.T. Jones Capital Equities Management violated a "safeguards rule" over a four-year period by failing to adopt any written policies and procedures to ensure the security and confidentiality of personally identifiable information and protect it from unauthorised access.

"The risk is there. Managers just need to decide the extent of that risk to their own organisation and take the necessary steps. Often when I'm talking to clients I tell them that there are two main reasons for data loss: bad guys and boneheads.

"A decade ago, throwing sensitive data away in the trash would have been careless but the breaches weren't so bad. Now, they can lead to far more serious breaches if you're not careful. The SEC's first exercise was really an information gathering one and I think they realised that financial organisations aren't that tight. I think we will start to see more exam findings, fines and actions coming from the SEC. The message is clear: the SEC is taking cybersecurity very seriously," says Doyle candidly.

Hedge fund managers have enough on their plates. They can be forgiven for thinking there is too much scaremongering going on.

And to an extent there is. But at the same time, managers need to keep on top of the issues and at least adopt a pragmatic approach to staying secure.

Take social engineering for example. This is a huge challenge for all businesses but by taking some straightforward, practical steps, safeguards can be put in place. This ultimately comes down to training and education.

Doyle says that in his experience, the problem is that a lot of the training is a bit dry and technical.

"Managers need to ensure that employees are being told clearly what the pertinent issues are and outline the situations when they need to raise their hand if something unusual is happening. That training needs to cover things like best practice in terms of creating strong passwords, changing them frequently, making them complex.

"The training also needs to focus on social engineering. It's an easy way to take of advantage of someone. People by their very nature are trusting. It's in our nature that when somebody calls, the assumption we make is that they are coming from a good place," comments Doyle, who outlines the four main steps that cyber criminals typically follow.

Step one starts with intelligence gathering. This involves looking at social networking sites, public records, which they will use to move on to the second step, which is developing a relationship.

They establish plausible scenarios that will allow them to earn someone's trust. Then they move to step three, which is to exploit the relationship to extract some form of value – maybe they masquerade as an LP to make a wire transfer – and then, step four, they flee.

"Sites like LinkedIn will allow them to quite easily determine whether a hedge fund manager uses an IT outsourcing company, for example. A cyber criminal would look at that and determine that it is likely they are working together, particularly if somebody posts a recommendation on LinkedIn. They might then call an employee at the hedge fund, pretend to be a staff member of the IT company, and say that they need to put a patch on their laptop to update their security by clicking on a specific website.

"Once the hedge fund employee does this and downloads the patch, the cyber criminal can take control of the laptop remotely," explains Doyle.

This is known as an "advanced persistent threat" ('APT') and allows the cyber criminal to build a detailed internal picture of a firm without anyone being aware of it.

In the US, with all the regulation that exists, companies must reveal in disclosure documents where their records are held if they are using a third party provider because the SEC requires it.

One of the things that firms need to understand is that these are expert criminal gangs and they only have to be right once.

"Kaspersky Labs wrote recently that the average return of a cyber criminal/hacker is 20 times their investment – that's a pretty good return!" says Doyle. He continues:

"Incidents of social engineering are on the rise. We've heard from clients that they have been attacked in this manner, particularly larger organisations where there is more data to find on individuals. Smaller fund managers still fall below the radar but there are, without doubt, so many ways that people will come after you to try to get your data.

"Still the biggest thing we hear from clients is the email phishing scheme. Someone internally gets their email account compromised, they get an email saying that funds need to be wired."

When that happens, which is pretty often, people just need to get on the phone to get a second opinion; go and speak to one of the IT team. Call the fund administrator – it sounds obvious but these incidents are designed to happen precisely when people are at their most vulnerable: end of the day, New Year's Eve perhaps when most of the senior staff are out of office.

Asked what fund managers can do to combat the threat of social engineering, Doyle stresses the point about staff training.

“A consistent message needs to be communicated, one that uses different scenarios. Too often, training tends to be too technical and does not consider scenarios. These are investment management experts, they are not cyber security experts. So whoever is conducting the training – the CTO, an outsourced consultancy – has to use practical examples. If someone looks at a file and thinks, ‘I didn’t make that change’, that could be a red flag.

“You then need to have in place proper procedures for giving out information. Make sure that employees confirm things over the phone. Emails are too passive,” concludes Doyle.

Tags :

- Technology and software solutions