

HEDGE FUNDS

REVIEW

Leading hedge funds assess threat from cyber criminals

Cyber attack alert

Author: [David Walker](#)

Source: [Hedge Funds Review](#) | 04 Jul 2011

Cyber attacks have become more frequent but so far hedge funds have not been a target. Nevertheless, many prominent hedge funds are assessing their defences and putting up defences against hackers.

Hackers recently attacked Sony, Lockheed Martin, broadcaster PBS and Nintendo.

Will hedge funds be their next target? This question is already exercising minds at some of the industry's most prominent managers.

Breaching technology networks has resurfaced as a growing concern for hedge fund managers amid recent allegations that a number of former employees of \$2.5 billion hedge fund Ikos illegally copied trading code. Those mentioned – in material Ikos distributed widely in May detailing its allegations – could not be contacted for comment.

The topic of IT security also arose at a recent client conference hosted by \$11 billion manager CQS. Chief executive Michael Hintze named cyber theft as one of the five concerns “that keep me awake at night. As managers of businesses, you have to be cautious. It is no longer about guys messing around in a dorm room.”

Hintze made no suggestion CQS had been targeted. Nevertheless, security consultants say cyber crime is already hitting some asset managers, including hedge funds. Alan Brill, senior managing director with risk consultancy Kroll, says he has three active projects with asset managers. He describes two as ‘post-incident’.

Consultants agree with Hintze's assessment. “When we've been asked by a client to look for something, we've generally found something,” comments Nik Whitfield, head of investment banking at IT security company Detica.

“There are run-of-the-mill defacers but the type the asset management industry has been concerned with is sponsored attackers provided with resources. Being in the financial industry, you attract a certain type of attacker,” notes Jim Tiller, vice president of security at BT.

Raids can be unified and designed to confuse, he says. They may target email, applications and internet connections simultaneously or separately.

Attacks may also be diabolically simple. One hacker placed house keys with a memory stick in a company's car park. When an innocent employee put the device into their work computer to find the owner's name, malware on the stick infected over 1,400 workstations and servers.

“Hackers are indiscriminate when it comes to industry. If they think they can get money from you, they will. Their attacks are extremely targeted and incredibly effective. The financial industry is getting hit every day,” Tiller says.

Despite this Jason Scharfman, managing partner of Corgentum Consulting, says information security is “extremely overlooked by hedge funds. They are information-driven organisations but with very basic controls in place to protect their information.”

Infiltrating the system of a model-driven fund could allow a hacker to place rogue trade orders without being detected. This would impact not only the company but also potentially the markets. Expect redemptions, lawsuits and regulatory anger in such instances.

Having systems and products to prevent this will be the next frontier of operational due diligence, according to Aleks Kins, CEO of AlphaMetrix. Having only commoditised safeguards such as firewalls and passwords in place will not be good enough.

Whitfield says the fact hedge funds are at the cutting edge of trading ideas makes them prime targets. “If someone were interested in stealing the latest and best trading ideas, a hedge fund would be a reasonable place to start.

“At the moment it would be easy to argue that hedge funds are more of a target than brokers. Before the recession there was a lot of proprietary trading activity going on on the sell side. Post-recession a lot of that has changed and banks see themselves more as client flow organisations. Prop trading has moved to the hedge funds,” he notes.

Security consultants say hedge funds think they are ‘too small to matter’. Kins says the industry’s relatively low profile has protected it to now. “However, as stories spread about the size of hedge funds, it will attract the attention of hackers,” he predicts.

Kroll’s Brill says hackers already realise they do not need to concentrate only on the largest asset managers to make good money. “Smart, mid-sized firms may be small in comparison to other businesses but in terms of what money, IP or inside information there is to steal, they’re just as valuable to bad guys [and] everyone is equally close to the bad guys.”

Storing information electronically – standard procedure at hedge funds – along with automated and algorithmic trading has precisely “encapsulated great trading ideas in well-defined code,” one consultant says.

Forecasts, business plans and customer lists can be as useful to a hacker as trading programs, according to security experts.

“More than ever before it is possible to reach inside an organisation and take that information out of it. For those reasons hedge funds should be cautious. They are being targeted for their crown jewels,” Whitfield says.

To guard against a threat managers must understand it. As cyber threats continuously evolve, Kroll’s Brill says managers must be able to adapt the measures they take to defend their networks as quickly as hackers find ways of attacking them.

Strengthen resilience to external attack is the advice of consultants. Just as importantly they advise managers to have a way to discover when attackers are already inside a system and also implement processes to reduce the possibility of employees or contractors stealing sensitive data.

“Attackers’ mindset has changed fundamentally in recent years,” says Brill. “Five years ago a typical attack was hit-and-run. Today the model is persistence: get in, dig deep and stay below the radar and keep active within the target’s systems for months, maybe years. As an attacker if you can stay active in the network, you get the opportunity to steal data or information, not just once but continuously,” he adds.

John Kindervag, senior analyst, security and risk management at Forrester Research, emphasises the importance of knowing when an attack happens.

Only 30% to 40% of people discover a breach when a third party finds it, he says. In cases where staff uncover threats, a system usually has already collapsed and damage has been done.

“In general people do not have control that goes deep enough or looks at the entire stream of the data or do not have controls that look at the visibility or what is happening in their internal networks. Once you breach the perimeter you often have free rein of the network,” notes Kindervag.

In its security work Detica looks in more detail at whether, for example, documents are being ferried out of organisations. “We try to get a thorough understanding of the data that is flowing into and out of an organisation at the most fundamental level possible. That allows you to run analytics across the data, and try to infer if there is activity going on you are not aware of, but should be aware of. It is at a fundamental level, not an application level, so looking at bytes rather than specific documents,” says Detica’s Whitfield.

He also encourages a culture of reporting things that seem wrong, and suggests considering banning memory sticks.

But according to Brill traders cannot be expected to focus on monitoring systems and understanding exactly how cyber threats against them may be changing. He also thinks small companies should not be expected to pay as much on defences as larger rivals. “Commercially reasonable security,” he says, is necessary. For him ‘reasonable’ is relative to the size of each company and how it uses technology.

For example, ‘zero day’ attacks, which have not been seen before, can be expensive to guard against. However, they are also expensive for hackers to conduct so they may not target smaller companies.

The popularity of cloud computing, particularly among small companies eager to tap into more computing power than they can afford themselves, could weaken security, consultants say. It may be seen as enabling quicker access to markets, new product suites and reduced expenditure.

Detica's Whitfield counsels those using the cloud to check which jurisdictions their sensitive data is being stored in and to have "a very firm understanding of the security capabilities and security levels being offered by suppliers. If any third party has access to any of your data, they have to be able to reassure you as a hedge fund they are taking measures to secure that data properly."

This includes prime brokers and custodians. "I am not sure how much of that is being specifically demanded by funds at the moment," he adds.

BT's Tiller says the number of external systems and mobile devices asset managers use can blur the definition of where a business's guarded perimeter fence actually is. "As you expand your mobility devices your target environment is expanding rapidly and becoming more integrated with your internal [IT] systems," he notes.

Ryan Rubin, director of security and privacy in the UK and Europe for risk and business consultants Protiviti, says one problem is younger employees are now technically savvy and typically regard it as natural to use iPads, smartphones and other remote devices to access company systems. They have also embraced social networking and increasingly rely on third-party services to provide data.

A generation accustomed to posting private information into public realms such as social networking sites may not be as sensitive to notions of protecting corporate data, he cautions.

While blanket bans on portable devices make little sense, he says there is software allowing IT departments to block or (better) control data being transferred onto devices. In some cases organisations can also delete software and data remotely when mobile devices are lost or stolen. He advises fund managers make sure staff report such losses quickly and are aware of security policies.

He recommends companies review guidance such as that provided in the UK Financial Services Authority's data security guidelines on safe practices as well as other industry good practices from standards such as the ISO27001 framework and payment card industry data security standard.

Powerful mobile devices with large storage capacities – from MP3 players to memory sticks – also make it easier for staff to steal data from their employer. Rubin says system controls can be put in place to record and in some cases limit the data taken or copied onto them.

Intellectual property (IP) in programs and electronic data can also be tagged based on their content using emerging technologies such as digital rights management, electronic watermarking and 'data leakage' tools. For example, these technologies can help ensure data cannot be used past a certain date or block data electronically tagged from leaving the organisation via email or mobile devices.

A company's uniquely marked datasets or programs make it easier to prove IP has been stolen if it finds its way to a competitor or into the public domain.

Regarding network access Rubin says the notion of 'least privilege' can be useful, giving people access only to systems and data they need for their job and limiting exposure to key information systems and sensitive data.

Kindervag says about half of attacks come from insiders and they can be more costly, given knowledge of systems, and what is most valuable.

Whitfield counsels chief risk officers to undertake standard precautions: check which employees and suppliers have physical access to rooms, and electronic access to systems. "Both awareness of internal and external threats is important," he counsels.

Kindervag says it is important to check every packet of data traversing networks and not separate a network into a 'trusted realm' and an un-trusted one. Even if someone is trustworthy, a hacker may use his or her access to the system.

"You have to change the trust model to 'zero trust' so every network is untrusted," notes Kindervag.

If fund managers want IT risk consultants to find perpetrators, they should understand this could become a traditional investigation or even a matter of law enforcement, particularly if they are trying to retrieve stolen goods.

If an 'inside job' is feared, Kroll's Brill says a traditional investigation might be needed. If it could lead to court, security companies will need to be well versed in proper handling of evidence right from the start of an incident.

Whitfield recommends greater co-ordination between hedge funds, possibly sending aggregated data on cyber attacks anonymously to a central point which could analyse it and report it to the industry. Although he thinks this a good idea, he does admit collaboration within the industry may be difficult.

“The financial industry is all about competitive advantage, so the levels of co-ordination and co-operation on these kinds of matters are low. We are speaking about standalone entities solely interested in competitive advantage,” he notes.

“But the chances are when one hedge fund is being attacked using a modern operation, then another one will be being attacked, too. The quicker you can share information on that, the faster the whole investigation into it could be,” concludes Brill. “Once you have consensus among that community, they can discover what the types of attacks are, so they would find it beneficial to share information.” ■

[Print](#) | [Close](#)

© Incisive Media Investments Limited 2010, Published by Incisive Financial Publishing Limited, Haymarket House, 28-29 Haymarket, London SW1Y 4RX, are companies registered in England and Wales with company registration numbers 04252091 & 04252093.