Cybersecurity for Hedge Funds 2015

How to establish Best Practices in cybersecurity
System integration has created security threat
Why cybersecurity needs to become a business issue
In this issue...

03 How to establish Best Practices in cybersecurity
By James Williams

06 SEC guidance on cybersecurity
Interview with Bob Guilbert, Eze Castle Integration

08 Developing a balanced approach to cybersecurity
Interview with James Tedman, ACA Aponix

11 System integration has created cyber threat
Interview with Gerhard Grueter, Lawson Conner

12 Cybersecurity trends in an ever-changing landscape
By James Williams

14 Cybersecurity risk is a business issue, not an IT issue
Interview with Carl Chapman, Capital Support
With cyber risks increasing year-on-year, and regulators such as the Securities and Exchange Commission (‘SEC’) taking an increasingly prominent role in assessing the preparedness of broker-dealers and registered investment advisors, establishing cybersecurity best practices is not only useful; it’s a necessity.

Cybersecurity is a complex web and as such there are many areas to consider. The best place for any manager to start is to take a step back and assess the risk of their overall business environment.

“It should be woven into business process and supported by senior management. It should not be relegated as being just an IT issue," says James Tedman, Managing Director, ACA Aponix (Europe). “It’s all very well having sound processes but you need to make sure you can evidence that. When it comes to risk assessment, firms should create and manage prioritised issue lists and demonstrate how they are working through these. They should maintain inventories of all devices, and create data maps, so that they can show where data resides and how it flows through the organisation and externally to vendors.”

Rather than cybersecurity becoming a Sisyphus-like challenge, managers can partner with outsourced technology specialists who spend their working days keeping on top of this ever-changing landscape. As Mike Asher, CIO, Richard Fleischman & Associates – a leading New York-based outsourced technology consultancy - comments: “Our R&D department is constantly testing new products to determine what is viable and what we should be paying attention to.”

“There’s no silver bullet solution. But at least managers should make a breach as
difficult as possible,” adds Grigoriy Milis, chief technology officer at RFA. “If it does occur, they need to know about it as soon as possible. Those are the two goals that we are trying to achieve for our clients, and which any hedge fund should try to accomplish.”

At a high level, Milis briefly summarises some of the key components to establishing a solid cybersecurity programme. Firstly, managers are advised to implement next generation firewall solutions “combined with a managed security service that can monitor the intrusion detection aspect of the firewall on a continuous basis”.

“Secondly, we recommend a next generation end point solution. End point still remains one of the most unprotected parts of any infrastructure in the hedge fund space. Regular detection rates with antivirus solutions are somewhere in the region of 35%, which is clearly not sufficient,” states Milis.

Thirdly, implement a data governance policy. This helps managers to not only identify sensitive information on the company’s servers but also shows who has access to that information; that can be an invaluable tool if they need to determine the extent of a cybersecurity breach event.

“We also recommend encryption solutions as the last line of defence to protect the most sensitive information in the company,” adds Milis.

**Data management & data fraud**

One of the best lines of defence in any cybersecurity programme is establishing a robust data management solution. Cybersecurity does not simply mean nefarious forces trying to infiltrate the network; it is also about data loss within the firm, which represents a significant reputational risk.

Hedge funds are unique in that they transfer data to multiple sources – their prime brokers, their fund administrators, etc – and as such it becomes a difficult task to keep track of that data and guard against data fraud or internal failings. “It’s important for hedge funds to understand exactly what data their service providers have access to, how and where this is stored, and how it is secured. That’s vital,” stresses Tedman.

Richard Anstey is CTO at Intralinks (EMEA). He points out that there is still an over-reliance on transmitting data via email and is an issue that needs addressing. There are technologies out there that can, in a relatively friction-free way, provide a more secure means of information transmission.

“Information Rights Management (IRM) is one such technology that we recommend for the transmission of any kind of secure information between parties,” says Anstey. “It can still be facilitated and notified by email but the actual delivery of data is secure. With IRM steps can be put in place to make it difficult for someone to print out information or photograph the screen by using watermarks in documentation.

“Moreover, you can remotely revoke access to the data at some later date. It’s like having an electronic remote version of a paper shredder. You can destroy data that you’ve shared with someone that you think is no longer relevant using IRM technology.”

**Vendor appraisal**

Vendors are often the firm’s weakest link when it comes to cyber risk. Firms should take heed of the FCA’s “Dear CEO” paper, which was released last year and apply a robust vendor management programme as part of cybersecurity management.

Not all hedge funds have sufficient visibility of processes within the vendors they partner with. SOC 2 and ISO 27001 are all perfectly valid certifications that are hard to earn “but we recommend to our clients that they go beyond that. They should build a clear understanding of the vendor, their process, people, and be comfortable that policies are being followed in practice,” comments Tedman.

In other words, managers shouldn’t take blind faith that their vendors – and this includes their key service providers such as prime brokers – are doing all that they
Cyber criminals are watching
Regulators are coming
Clients are asking
Are You Prepared?

Cybersecurity threats are intensifying. Your security posture must be comprehensive and complete with Administrative, Physical and Technical Safeguards. Eze Castle Integration can help - Let us:

- Develop your Written Information Cybersecurity Plan
- Move you to the industry’s most secure Private Cloud
- Fortify your existing IT environment

Contact us at 800 752 1382 (US) or 0207 071 6802 (UK)
visit us at www.eci.com

BOSTON | CHICAGO | DALLAS | HONG KONG | LONDON | LOS ANGELES | MINNEAPOLIS
NEW YORK | SAN FRANCISCO | SINGAPORE | STAMFORD
Cybercrime could extract up to 20 per cent of the global economic value created by the Internet through fraud and espionage, according to the Centre for Strategic and International Studies. Following last year’s Cyber-Security Risk Alert, the SEC’s Division of Investment Management released guidance this April to help investment managers prevent external attacks.

“The guidance can be boiled down into three key areas of recommendation: assessment, strategy and implementation,” says Bob Guilbert. Managing Director at Eze Castle Integration, the leading provider of IT solutions and private cloud services to more than 650 global alternative fund managers.

Guilbert outlines the first area that managers should focus on: assessment. “The SEC has identified five areas that should be addressed on a periodic basis. Those five areas are:

- **The nature and sensitivity of confidential information:** Where is it located, how is it used, what systems are used by it? This could include investor and employee personal information, as well as fund information and company financials.
- **The cybersecurity landscape:** It is ever-changing and managers need to ask: What are the current threats? What are the firm’s specific vulnerabilities within that changing landscape? As part of that, Eze Castle Integration recommends a technical policy assessment to identify areas for improvement.
- **Security controls and processes:** Firms should review access control policies, specifically looking at which employees have access to what information, etc.
- **Impact:** What type of impact would your firm potentially see were there to be a security breach?
- **The effectiveness of a firm’s governance programme in terms of managing cybersecurity risk:** In other words, who is responsible for managing the security risks?

Does the firm have a Chief Information Security Officer (CISO) in place? Or an incident response team?” explains Guilbert. For the second area of focus - cybersecurity strategy - again there are five key considerations:

- **Access controls:** using systems with identification and authorisation methods including firewalls and perimeter fences. “This is about employing layers of security across all aspects of the firm’s technology,” says Guilbert. “For example, putting in place authentication limits to control who has access to what information and validating how people access third party data sources.”
- **Data encryption:** determining where and when encryption systems should be used (e.g. should mobile devices be encrypted?).
- **Removable storage media:** firms should have a lockdown strategy to prevent the copying and transfer of confidential or critical files in or out of the organisation.
- **Backup and retrieval:** “What strategy does the firm have to recover and access backup files? How often are backup tests performed? Who is responsible for managing this process?” adds Guilbert.
- **Incident response plans:** Establish guidelines to respond to a particular security incident and outline who is responsible for managing the response process.

“The third area of guidance is implementation, specifically having proper policies and procedures in place,” notes Guilbert. “The biggest takeaway here is that managers need to have a Written Information Security Plan (WISP) and employee cybersecurity training practices in place. The WISP should be in place to protect a hedge fund’s confidential information and uphold the integrity of that information. It should be reviewed periodically and shared with investors when requested.”
can to uphold the security and integrity of a fund’s data. Rather than take their word for it, managers should seek independent verification.

“One telling statistic is that 69 per cent of breaches are detected by an external party (Mandiant M-Trends 2015). This highlights the value of an independent audit – you can’t check your own homework. It does not mean that the IT team or service provider is doing a bad job, it’s just that an extra set of eyes gives independence and avoids conflict of interest,” says Tedman, adding:

“Reviews should be undertaken at least annually and the questions that you ask of your vendors should be tailored to the role that they play and the data that they are privy to. Use searching questions that avoid simple Yes or No answers.”

RFA’s Asher points out that prime brokers are working hard to identify the weakest links and establish secure communications with all their clients; partly because many have been breached already, partly because they do not want to suffer any further reputational damage.

“They are providing alternative asset managers with helpful questionnaires that can be shared with their vendors to make sure they are compliant with SEC guidelines, as well as providing guidance on what firms need to do to secure themselves to an acceptable baseline level,” says Asher.

Bob Guilbert is Managing Director at Eze Castle Integration. In his opinion, the vetting of third party vendors is becoming essential; not only as best practice, but also because investors themselves want to know what business continuity plans and incident response plans these vendors have in place.

“Investors are getting a lot more savvy and asking detailed questions to ensure that the end providers themselves have the proper cybersecurity plans in place as well as the manager.

Asking questions on BCPs, etc, should become a thorough part of a manager’s own due diligence process when selecting their service providers. Thereafter, the manager should conduct annual due diligence checks. We advocate going to visit them in person. For example, we use top-tier data centres for the protection of the Eze Private Cloud and we encourage clients to go and visit one as part of their annual periodic review.

“IRM is one such technology that we recommend for the transmission of any kind of secure information between parties. It can still be facilitated and notified by email but the actual delivery of data is secure.”

Richard Anstey, Intralinks

“We ourselves are constantly making adjustments to respond to this changing landscape. The funds themselves should be asking for updated BCPs and updated WISPs, to reflect this changing landscape,” comments Guilbert.

Written policies

Establishing cybersecurity best practices should not only be about prevention from external threats but having the necessary internal policies and procedures to recover from a breach attack. This should not be confined to the minds of the CTO or senior IT staff; rather, firms should look to build out an incident response plan.

In a white paper written by Capital Support Limited in May 2015 entitled Cybersecurity Threats and Vulnerabilities, they point out that an IR plan should include the following six components:

• Incident classification
• Data classification
• Performance targets
• Operating models
• Identify weaknesses
• Tools and guidelines.

Asher states that confusion arises within hedge funds when it comes to understanding what needs to be done when a breach occurs and how it should fall into the manager’s overall business continuity plan (BCP).

“There’s no hesitation invoking a disaster recovery component when there’s a technology issue i.e. a power outage. It’s a well-defined practice. But reporting a cybersecurity breach to a third party vendor that might then be required to relay information during a regulatory investigation means that there is still hesitation. It is
Developing a balanced approach to cybersecurity

Interview with James Tedman

There is a tendency when faced with a potentially serious threat to take extreme measures in life. Cybersecurity is no different. Many firms are looking for a quick fix, even if it comes with a high price tag. However, should managers take a more balanced and common sense approach to tackling the issue of cybersecurity, before spending vital operating capital on expensive individual solutions?

“Frequently, hedge funds are led to believe that the best way to protect themselves against cyber threats is to invest in expensive intrusion detection systems (IDS) or sophisticated firewalls,” says James Tedman, Managing Director, ACA Aponix (Europe). “These items are effective, but it is important to understand their role and limitations. Rather than a silver bullet solution to the problem, they should be considered as one component of a balanced cybersecurity risk programme.”

To develop a balanced response, managers need to first assess risk – understand the threats posed as well as identify vulnerabilities within their business process and technology.

“The published findings of the SEC OCIE sweeps stated that 79 per cent of the investment advisers surveyed had carried out risk assessments. However, we see that few managers undertake a true risk assessment and that many consider a network perimeter penetration test sufficient for identifying risks. A risk assessment should be a broad review that encompasses all aspects of the business and technology. A penetration test will not highlight whether a firm is using unencrypted email to communicate with their fund administrator or reveal an issue with the management of data backups,” notes Tedman.

The first step in any risk assessment is to build an accurate picture of the environment. This includes knowing what devices and software are being used. Also, what data exists in the environment, where it is stored, how it gets there, who has access to it and how it is secured.

“It is important to create and maintain up-to-date inventories; this process can be automated using software to catalogue devices and software. On the data side, you should be able to map out where data resides both inside and outside your infrastructure. You should know what this data is, how critical or sensitive it is, and how it gets there. This will not only help to determine where to focus your effort in terms of implementing security measures, it is also essential information when trying to remediate a breach,” explains Tedman.

Given the trend towards outsourcing in the hedge fund sector over recent years, and the amount of sensitive and business critical data to which vendors are privy, they can also be a significant security risk. Recent examples of this are the Target and US Office of Personnel Management (OPM) breaches where credentials were stolen from contractors.

As Tedman points out: “All managers should have some form of vendor management programme with each vendor assigned a risk classification based on their role and data access. Firms should be undertaking deep due diligence on key vendors to get a detailed understanding of their process and security measures. Other items to consider are security on the transport mechanisms used to send and receive data to vendors, as well as including specific provisions for cybersecurity in third party contracts.”

By taking a bottom-up approach to assessing risk in the environment, managers can develop a more effective cybersecurity framework. “It is about identifying weaknesses in a fund manager’s technology, their processes, their vendor relationships, and within their staffing arrangements as well. It needs to be a broad, balanced assessment of their environment,” concludes Tedman.
uncharted territory and that’s where the confusion stems from.

“It’s an educational process from our end, explaining what needs to be included as part of a comprehensive business continuity plan that is actionable and allows the manager to proceed with their operations even if a breach is detected,” says Asher.

One document that is becoming an important tool is the Written Information Security Plan (WISP). As Guilbert explains: “The WISP covers both administrative and technical safeguards as well as the incident response plan, third party risk assessments and employee guidelines. It allows us to look through all facets of a hedge fund manager’s operations, from a cybersecurity perspective.

“The WISP should be periodically reviewed and shared with investors when requested.”

Recently, the SEC found that 83 per cent of advisors have adopted a WISP but Tedman warns that not all of them pass muster. Typically, he says, there is minimal data governance, the incident response plan is weak or non-existent, and all too often the WISP template has simply been lifted off the internet.

“Policies should be specific to the organisation and based upon a deep understanding of the environment such that they are practical and demonstrable as well.

“They should, in short, reflect the culture of the firm. Going forward we expect to see much more interrogation of security processes with regulators looking for clear evidence that firms are adhering to best practices, not just asking them whether they are or not,” says Tedman.

**Staff training**
The majority of cybersecurity issues that arise are preventable and typically result from human error. As such, training and educating staff are an obvious way to mitigating this risk. As Guilbert states, the first line of defence is “preparedness, awareness and education”. “It’s the concept of having multiple locks on the door to dissuade potential cyber hackers. We are seeing more attacks happening at the individual level through phishing attacks and targeted phone calls. Padlocking the door means properly educating employees as to who is responsible for validating emails, using tools to validate email links, looking at phishing attempts and teaching sound practices on avoiding social engineering techniques,” says Guilbert.

Anstey points out that one of the strengths of information rights management is that it means managers have a technology solution in place that help them to recover from accidental data loss. “The advantage of IRM is that you retain control even after the content has left the organisation,” says Anstey.

Tedman says that staff training is a major issue, noting that the vast majority of attacks involve some form of phishing or social engineering as this is the easiest route into an organisation.

“Building staff awareness of cybersecurity threats and educating them on best practices is extremely important and will substantially reduce a firm’s vulnerability to attack. As part of our process we run employee training sessions and phishing tests. In the phishing tests we undertake with our clients, we are typically able to harvest around 40 per cent of the user’s credentials and gain access to email or the file system.”

By thinking about some of the above considerations managers will better understand their threat matrix and be able to create solutions to address the most likely attack scenario.

As Milis concludes: “It’s being cognizant that the landscape is changing and the need to take proactive measures to stay protected.”
Lawson Conner
Compliance. In safe hands.

- AIFMD Solutions & Hosting Platform
- Delegated Risk / Portfolio Management
- Compliance Assessment and Regulatory Support
- Risk Advisory & Monitoring
- Compliance Outsourcing

For more information please contact:
Daniel Maycock
dmaycock@lawsonconner.com
London: +44 207 305 5810
New York: +1 212 5379095
Hong Kong: +852 2165 4109
Boston: +1 617 207 4116
lawsonconner.com
Today’s world has never been more interwoven. Cybersecurity risks have grown exponentially as global businesses have become more integrated with counterparties and system architectures have grown in complexity. In the opinion of Gerhard Grueter, co-founder of Lawson Conner, a market leader in compliance solutions for the investment fund industry, the topic is only going to get bigger.

“Today, cybersecurity has become a genuine commercial issue that can bring down entire firms because of reputation risk and regulatory risk. The threat today is nothing like what it was five years ago. It is now an active market of cyber criminals deliberately going after data and attacking firms that have become much more integrated,” says Grueter.

One of the problems unique to hedge funds is that they are perpetually engaged in data sharing and have multi level "access" points across numerous jurisdictions - be it with their prime broker(s), their fund administrator, other critical data and software providers. This flow of “Big Data” across multiple nodes means that hedge funds have a potentially higher number of weak points for cyber hackers to target.

“A fund manager ten years ago was an island in terms of technology,” says Grueter."They used a few disparate systems and all of the solutions were quite singular in nature. Now, these solutions have become completely integrated. This means that if one system goes down, it could bring down the entire platform. Moreover, managers are not only dealing with one counterparty, but multiple counterparties who themselves delegate responsibilities to counterparties that the manager doesn’t even know of.

“The industry has created some kind of a monster and nobody has said, ‘Hang on, let’s look at this and see if we can’t make things more secure.’”

Those most vulnerable to cyber threats are smaller managers who do not have the budgets to afford full-time IT specialists. Even for those who do, there aren’t enough internal resources to allow IT teams to plan for non-standard situations.

“This is putting demands on IT teams to not only administrate the network but to become cybersecurity specialists. Managers need to give IT a bigger focus and allocate more budget to deal with the unseen threat of cybersecurity risk – just the same as the COO has to deal with operational risk,” suggests Grueter.

To overcome the burden of acquiring in-house cybersecurity expertise, firms like Lawson Conner are able to manage the threat as part of a wider outsourced compliance function; welding together a hedge fund’s internal expertise with external specialist cybersecurity expertise.

There are two areas in which Lawson Conner helps clients. “One is for clients on our investment manager platform who benefit from a standardised approach to cybersecurity: testing, monitoring, risk assessment and finding gaps. Managers can outsource a large proportion of their cybersecurity risk and compliance to our specialists who are not only doing this on behalf of one client, but multiple clients.

“The second area is for new funds who aren’t on our platform, yet don’t have the ability to hire a specialist IT person full-time. In this context, cybersecurity forms part of our outsourced compliance service. This is an ongoing service requirement as opposed to being a consultancy service, which is finite. And that’s critical given the fact that the cybersecurity threat is constantly evolving,” concludes Grueter.
Hedge funds are an integral part of the financial fabric, and, whilst they may not have the same capital profile as large investment banks, the Bank of England is advising that they strengthen their resilience in order to recover quickly from attacks.

In the Bank of England’s July 2015 Financial Stability Report, they write: “A successful attack on a systemic institution or vital infrastructure (including non-financial infrastructure that the financial sector relies on, such as utilities) could cascade throughout the financial system.”

In May 2014, the BoE established a vulnerability testing framework – CBEST. Although this is aimed primarily at banking groups, the largest hedge funds that could present a systemic risk to the UK economy should be adopting similar defensive measures.

“We are seeing new advances in the way these attacks are being carried out and determining their origin is becoming increasingly difficult,” says Matthew Martindale, director, KPMG’s cybersecurity team. “Cyber is another vector for the kinds of attacks that have been happening for many years - hactivists will launch physical attacks on buildings but the internet gives them anonymity.”

Sophistication of attacks
One of the clearest cybersecurity trends is the sophistication of attacks. In December 2013, the CFO of hedge fund group Fortelus Capital Management LLP received a phone call late Friday afternoon, just as he was leaving the office. The caller pretended to be from Coutts, the hedge fund’s bank, and the net result was that USD1.2 million
Cyber Secure

A tailored suite of cybersecurity services developed by Capital Support to enhance our customers' security provisioning.

Cyber Secure Protect and Detect
From dual layer firewalls to traffic monitoring, Cyber Secure Protect and Detect provides next generation firewall functionality that prevents imminent cyber-attacks from breaching your systems.

Cyber Secure SIEM
Cyber Secure SIEM (Security Information and Event Management) is an extension of the Protect and Detect service, with SLA-driven log analysis and alerting, managed by security professionals from an advanced 24/7 Security Operations Centre.

Security Risk Management
The second element of our Managed Security services is Security Risk Management, which provides guidance and support to help our customers meet regulatory standards. We use our ISO 27001:2013 accreditation to help fill gaps in your business security provisions.

ISO 27001:2013 Accredited
Earlier this year Capital Support received its ISO 27001:2013 security standard accreditation. This provides our customers with reassurance of our dedication to information security and shows how seriously we take the protection of their data.

For more information on Cyber Secure or any of our other services, please get in touch.

PROTECT YOUR BUSINESS
020 7458 1250
info@capitalsupport.com
www.capitalsupport.com

THE MOST TRUSTED & RESPECTED IT PROVIDER
Cybercrime is building to tsunami-like proportions and hedge fund managers are not immune from the threat yet there still appears to be a degree of naivety.

According to Carl Chapman, COO of Capital Support, a leading managed IT services provider, C-level executives tend to overlook the importance of having a solid security risk programme. “They still think cybersecurity is an IT issue but it’s not; it’s a business issue.

“One of the approaches we’ve taken with some of our customers is to explain that cybersecurity is really just risk management and should be treated in the same way as trading risk and operational risk in the middle and back office,” says Chapman.

“If you mirror the same process and call it "security risk management" rather than risk management, then effectively you are retaining the understanding of terminology, which the CEO can relate to,” says Chapman.

“Our responsibility is to help fund managers with their choices. With any risk, you can choose to accept it or not. Allowing users access to their USB, for example, may be an acceptable risk but you can only accept that risk if you understand what the potential impact might be.”

Hedge funds are unique in that many trade with a greater sophistication than investment banks yet they may only have a dozen employees, a modest amount of AUM, and a far smaller IT budget. This makes cybersecurity a tricky balancing act whereby managers need to assess the cost of protection; how much should they spend vis-à-vis the threat level?

As long as firms understand the risks, Chapman’s point is that they can choose whether to mitigate them or not. One of the biggest risks that firms face is the inability to trade because of a virus entering their environment. Some, like the “Heartbleed” virus last year, enabled hackers to steal sensitive data and eavesdrop on users, as well as mimic them.

Then there’s CryptoLocker, a ransomware Trojan that encrypts data and sends an email along the lines of “Pay USD500 and we’ll give you the key to unencrypt the virus or else the data will be lost”. This isn’t exactly going to bring down a hedge fund, but as Heartbleed showed, the biggest threat to any firm is the ease with which they target the weakest link.

“Currently, there is no need for organisations to report such a breach to the regulator but in the same way that the US has disclosure rules, the FCA will soon require organisations to disclose any incidents that prevent them from trading – which could result in reputational damage to the manager,” comments Chapman.

The solution, says Chapman, is to look at the footprint of what could cause the threat in the first place and then mitigate it. Indeed, Capital Support is able to provide its hedge fund clients with access to a security officer who can independently provide advice and guidance, identify risks and help prioritise those risks when the manager chooses to mitigate them.

“Treat security risk as you would any other risk in your business. Once you understand the potential risk and impact, only then can you make smart business decisions about what you should mitigate,” concludes Chapman.
of fund assets were misappropriated. It was, unfortunately, a classic case of social engineering.

“There are attacks every day and you don’t have to be big; in fact, hackers prefer smaller, less defended groups,” says Eldon Sprickerhoff, founder and chief security strategist for the Canadian network-security company eSentire Inc. “We are seeing a doubling of cyber attacks year after year across our client base. The Fortelus attack wasn’t random. It was properly researched and executed according to plan. I’m sure it wasn’t the only RIA that was probed and targeted in this manner.”

Aside from social engineering, cyber groups are taking a more strategic, long-term approach to infiltrating networks and gathering sensitive information. The industry term is an “Advanced Persistent Threat” and it underscores just how careful fund managers must be at protecting their businesses. One cyber group that was identified by Kaspersky Labs in February 2015 was Carbanak.

“The basic idea of an APT is to infiltrate the system, disable antivirus, and quietly stay connected below the radar, gather keystrokes (conceivably including bank account details, SecureID details, and passwords) and use that information to pivot across different systems within the network. Over the long term, the cyber group essentially has remote control over the network and work out how best to extract value from the target organisation – and normally, that value is cash from either trading accounts or from working capital accounts,” explains Sprickerhoff.

By using signals intelligence, eSentire looks for “indicators of compromise” to determine if malicious attacks are occurring. “I try to describe what we do as providing an embedded incident response. If we see an attack on one client we step in to block them from all other eSentire clients. We’re constantly looking for new IOCs. We let clients know when traffic is being blocked to put them on a higher level of alert and we also send out regular advisories when broad cybersecurity attacks or issues arise,” says Sprickerhoff.

The two main modules it uses are EXEcutioner and Asset Manager Protect (AMP). The former provides white listing to prevent the download of malicious payloads; executables are one of the most common ways of downloading malware. If an executable is not on the white list, EXEcutioner shoots it down. The latter, AMP, is a black listing module whereby eSentire continuously scans the environment to block unwanted traffic.

Carl Chapman is the COO of Capital Support, a leading managed IT services provider. He says that if one looks at the lowest common denominator with cyber attacks, what cyber criminals are looking for is:

• A process that doesn’t have sufficient checks and balances
• An individual that is more trusting than they perhaps should be.

“If you can infiltrate a hedge fund with a cryptolocker-type virus and identify a vulnerability within the organisation then you can target it with a more sophisticated attack,” says Chapman, adding that the solution is to reduce the likelihood as much as possible.

“There are lots of different things managers can do to mitigate the risk of someone stealing valuable data from their network. But there’s no point locking the front door and leaving the windows open. This is risk management 101, it’s a straightforward business issue, and the only way to resolve it is by having an organisation’s people, processes and technology working in harmony.”

Social media
The parabolic rise of using social media in recent years has created a potential Pandora’s Box for hedge fund managers. On the one hand, developing a strong social...
No one understands the security concerns of the hedge fund industry better than Options. Our offering combines best practice cybersecurity building blocks with continued operational agility and rigour.

As cyber attacks evolve, both in number and sophistication, the SOC accredited Options platform can offer your firm lasting peace of mind. Visit options-it.com for more information.

Options is the leading managed service & IT infrastructure provider to the global hedge fund industry.

Cybersecurity in 2015: Is your firm ready?
media presence is necessary for managers to build their brand. But on the other hand, if Facebook and Twitter are misused, they could expose the manager to even greater cyber risks moving forward.

“Personally, one trend I think we’ll see more of is spear phishing attacks. If I wanted to send a clever phishing email I could go to LinkedIn, see who you work with, find out a bit about yourself, and I’d send you a nice email pretending to be one of your work colleagues to ask if you want to go VIP to a concert. They’d click on the link and that would initiate a virus. It’s that easy,” warns Chapman.

KPMG’s Martindale suggests that those managers who don’t embrace social media are potentially at risk from impersonations – something that could be catastrophic if investors receive inappropriate content.

“We run a series of simulated cyber exercises to help our clients prepare for a potential cyber breach and one of those often used is where we say that the Manager’s Twitter account has been compromised,” says Martindale. It’s an important point. After all, a portfolio manager – or someone pretending to be them – who shares thoughts on certain stock could potentially move its price.

**Understanding the data framework**

One trend that is likely to gain momentum, is managers focusing on prevention by understanding data within funds. For too long, CTOs haven’t necessarily kept tabs on what the finance side has been doing regarding strategies and data domiciled.

“The end goal is to understand what data you have in order to defend it properly. There’s no tech solution to that,” comments Sprickerhoff.

It’s important for CTOs to be aware of the pockets of data they have both in their enterprise and outside (e.g. within a cloud environment) in order to defend it properly, according to Sprickerhoff, who says: “Often data is shipped offsite to a public cloud that requires higher rigor than it’s given. It’s critical that this kind of “Shadow IT” needs to be controlled so as to not run afoul of regulations.”

Managers who can demonstrate that they have a robust cyber risk programme will also likely stand out from those who do not; in other words, just as operational risk and compliance are key issues for institutional investors, cyber risk will likely also become a criteria in manager selection.

“We did a survey recently and around 79 per cent of institutional investors said they would be concerned with their investments if any of the managers suffered a cyber breach,” confirms Martindale. “Those managers who can embrace the opportunity will be well positioned – and it’s not about rolling out the red carpet and waving your certification to say ‘we’ve done this’, it’s about truly getting a grip of your risk position. Be proactive; don’t just wait for regulation.”

**Outsourcing to cyber specialists**

Of course, not all managers have the IT budgets to shore up their technology network. Given that cyber risk has become a threat seemingly overnight, smaller managers face a challenge striking the right balance between budget and risk.

“It’s not about implementing security measures; you then need to maintain them,” says Gerhard Grueter, co-founder of Lawson Conner, a market leader in compliance solutions for the investment fund industry. “It needs to become part of the business fabric. Policies need to be tested, updated periodically, to see whether they really are as secure as they think they are. We can provide cyber risk expertise to managers as and when they need it as a trusted outsourced partner.”

For those who have robust cybersecurity policies and procedures in place they will have a competitive advantage, "not

“There are attacks every day and you don’t have to be big; in fact, hackers prefer smaller, less defended groups. We are seeing a doubling of cyber attacks year after year across our client base.”

Eldon Sprickerhoff, eSentire Inc
to be aware of (the other three are cyber assessment, strategy and implementation).

“I’d estimate that at most three out of 100 RIAs have hired a CISO. These firms typically have more than USD15 billion in AUM. One point that came out of our meetings with the SEC in the last year is that it’s not their intention to mandate that every fund must have a separate CISO designated.

“For funds under USD2 billion AUM, it’s more likely that the CTO and CCO will collaborate to cover the responsibilities usually given to a CISO, and will outsource the technical aspect to meet any remaining requirements. Why? Because the SEC compliance obligation for cybersecurity requires a new level of appreciation for cybersecurity rather than a new position. This is not wholly a technology fix. The SEC has specified that a fund’s General Counsel and CCO will need to understand their cybersecurity compliance legal obligations. It will be their duty to work with the CTO to ensure that adequate protection that is appropriate to the firm’s data, domicile, and strategy is implemented,” says Sprickerhoff.

To help managers assess what cyber risk measures to employ, eSentire has created a cybersecurity guidance matrix, released in their June 2015 cybersecurity advisory: www2.esentire.com/SECMatrix.

Detect and respond

Going forward, Martindale thinks hedge funds will increasingly look to improve their detection and response capabilities; something that is already seen in other parts of the financial industry: “In the detection space I use the analogy of alarming one’s house. If someone breaks in through the bathroom window, the right alarm needs to go off in the right room as quick as possible and the right level of response needs to be taken to contain that breach and recover promptly.

“However, this requires understanding where the threats are coming from. Managers should run simulated exercises to practice what they would do and what decisions they would make. Those who can respond and recover in a positive way from a cyber breach will come out in a positive light by mitigating the impact on stakeholders and investors.”