The threat within: Mitigating insider risk

Implications of data protection regs under Brexit

How to recover from a ransomware attack
In this issue...

03 Cybersecurity strategies for investors and managers
By James Williams

05 Protecting data through an audited cyber assessment
Interview with George Ralph, Richard Fleischman & Associates

08 The threat within: Mitigating insider risk
Interview with Mark Coriaty, Eze Castle Integration

11 The implications of data protection regulation under Brexit
Interview with Marcus Lewis, Capital Support

13 Low cost, liquid exposure to cybersecurity sector
Interview with Rahul Bhushan, ETF Securities

14 Cybersecurity innovation is alive and kicking
By James Williams

17 How to recover from a ransomware attack
Interview with Warren Finkel, ACE IT Solutions & Carrie Reber, Datto

20 Cybersecurity a top priority
By Castle Hall Alternatives

23 Cyber attacks: Prepare, respond and recover
Interview with Jason Elmer & Brian Lozada, Duff & Phelps

Publisher
Managing Editor: James Williams, james.williams@globalfundmedia.com
Managing Editor (Wealth Adviser, etfexpress & AlphaQ): Beverly Chandler, beverly.chandler@globalfundmedia.com; Online News Editor: Mark Kitchen, mark.kitchen@globalfundmedia.com
Deputy Online News Editor: Leah Cunningham, leah.cunningham@globalfundmedia.com
Online News Editor: Mark Kitchen, mark.kitchen@globalfundmedia.com
Graphic Design: Siobhan Brownlow, siobhan.brownlow@globalfundmedia.com
Sales Managers: Simon Broch, simon.broch@globalfundmedia.com;
Malcolm Dunn, malcolm.dunn@globalfundmedia.com
Marketing Administrator: Marion Fullerton, marion.fullerton@globalfundmedia.com
Head of Events: Katie Gopal, katie.gopal@globalfundmedia.com
Head of Awards Research: Mary Gopalan, mary.gopalan@globalfundmedia.com
Chief Operating Officer: Oliver Bradley, oliver.bradley@globalfundmedia.com
Chairman & Publisher: Sunil Gopalan, sunil.gopalan@globalfundmedia.com
Photographs: iStock photo
Published by: GFM Ltd. Floor One, Liberation Station, St Helier, Jersey JE2 3AS, Channel Islands
Tel: +44 (0)1534 719780 Website: www.globalfundmedia.com

© Copyright 2016 GFM Ltd. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the publisher.

Investment Warning: The information provided in this publication should not form the sole basis of any investment decision. No investment decision should be made in relation to any of the information provided other than on the advice of a professional financial advisor. Past performance is no guarantee of future results. The value and income derived from investments can go down as well as up.
Cybersecurity strategies for investors and managers

By James Williams

Whilst the cybersecurity narrative typically tends to focus on how asset managers are putting steps in place to improve their cyber preparedness, of equal importance is how investors can assess managers objectively as part of their due diligence process.

Bringing that objectivity is sometimes overlooked. Investors might be interested to hear about how managers are tackling the problem, but they need a way to scorecard them. To help with this, Castle Hall Alternatives has launched Due Diligence University to support asset owners as they conduct due diligence on third party asset managers.

The first white paper, in what will become a series of educational resources for investors, is entitled *Evaluating an Asset Manager’s Cybersecurity Environment*, which identifies ten key due diligence risk areas related to technology security and includes a cyber risk management evaluation tool.

“While there may be a gold standard for an asset manager that has significant internal resources to deploy, naturally that same gold standard cannot apply to all asset managers. As such, any assessment needs to include baseline aspects to a cyber risk framework that an investor could apply as a ‘common standard’ to all asset managers,” explains Daryl Purdy, Vice President, Castle Hall Alternatives.

Whilst it is fair to say that there is now a general willingness within the fund management industry to accept that proper policies and procedures need to be in place, there will inevitably be a wide range of capabilities among fund managers.

This year, both the National Futures Association and the Securities Exchange Commission have become increasingly active in assessing the ‘cyber preparedness’ of registered investment advisers, using
specialist IT teams to conduct audits. But whereas large institutional managers have not waited for the regulatory response, with many putting in place measures to beef up their cyber risk frameworks over the last couple of years, smaller managers are still in the early stages of implementation.

“Our risk evaluation tool serves as a framework to ascertain how prepared a manager is and use it as a basis for discussion whereby investors can share their initial thoughts on where they think the manager’s cyber risk approach needs to be improved. This is really a guidance tool. Through our ODD process we can also help managers move towards best practices and improve their business and operations,” explains Vladimir Rabotka, Director, Security and Systems Administration, Castle Hall Alternatives.

“We will come in and speak to managers about particular sections of the evaluation. I believe in terms of self-assessment it is a useful tool to have as it can help managers to work towards a position of being proactive rather than reactive, and stay one step ahead to identify which controls need to be in place.”

One of the 10 evaluation items is Data Classification. This, says Rabotka, is about understanding what constitutes sensitive information and how it propagates throughout the manager’s environment i.e. having a good idea of where data is being transferred, processed and stored in order for the manager to put in place the appropriate security controls. “Security controls always have to travel with the data,” says Rabotka. He says that an example of where this might be regarded as sub-standard in the investor’s eyes would be if there is no awareness over where such sensitive data is stored.

“For example, a manager that relies on vendors and consultants but doesn’t understand how much access these third parties have to their data, which might include investor data. Blind faith is put in third parties without having a clear and full picture of what exactly is being handed over and what level of access is being granted,” comments Rabotka.

If senior management within a fund group are providing different answers on where they think sensitive data is being held, and what the nature of that sensitive data is, this could point to a lack of Security Awareness and Training within the organisation; another of the 10 evaluation items.

“There are three types of sensitive assets that we typically see with our clients,” says Brian Lozada, Managing Director of Duff & Phelps’ Cybersecurity practice. “These include: 1. Investor data (bank details, names, social security numbers), 2. Employee data, and 3. Intellectual Property: trading strategies, algorithms, research notes.”

Vendor due diligence
To help managers reduce the cyber risks of using third parties, Duff & Phelps assess every third party who is either storing, processing or transmitting sensitive data on behalf of the fund and then look to ascertain exactly what that third party is doing from a security perspective.

“What controls do they have in place? Do they have a 24/7 response team? Does the third party have an Incident Response Plan? Does it go through vulnerability and penetration tests? Does it share those results with the fund? We ask a series of questions on their data handling processes and their recovery efforts in the event that they are compromised,” explains Jason Elmer, Lozada’s colleague and fellow Managing Director.

One of the issues that fund managers need to be mindful of with respect to their third parties is that if they have had contractual relationships in place for four, five years, they are unlikely to contain information security provisions.

With every new contract that is put in place, Duff & Phelps will help its clients to stipulate the information security provisions and breach disclosure terms that need to go in to the contract.

“Blind faith is put in third parties without having a clear and full picture of what exactly is being handed over and what level of access is being granted.”

Vladimir Rabotka, Castle Hall Alternatives
Protecting data through an audited cyber assessment

Interview with George Ralph

RFA (Richard Fleischman & Associates) is a leading technology and financial private cloud provider for the asset management industry supporting more than 500 global private equity, hedge fund, fund-of-fund and investment management firms.

To help organisations remain cyber secure RFA is able to advise on documented policies and procedures, technology solutions, as well as provide threat management to mitigate cyber risks.

“We have a set of policies that we create for our clients at the onboarding stage. These cover things such as disaster recovery, the vendor management process (understanding the complete supply chain when using third party IT vendors/cloud providers), as well as equip clients with the correct information for their investors so that they are able to answer cyber-related questions themselves with full knowledge.

“What we find is that some managers bring their IT specialist with them to investor meetings, which puts investors off because if you are the COO you should know everything about the firm’s technology,” comments George Ralph, Managing Director of RFA in London.

For start-up managers, this highly regulated environment can all appear quite overwhelming; indeed, in 2018, the EU is poised to introduce General Data Protection Regulation (‘GDPR’), which will place even greater emphasis on firms to protect data and demonstrate proper compliance.

To help its clients implement sensible best practices, RFA has developed a risk management process that highlights between 20 and 30 technology risks in any given organisation, the results of which are then provided to the fund’s board of directors.

“This means they have regular information on what the main risks are, what mitigating actions are being taken by the manager, and they can talk through those with the fund’s investors. Outside of the finance sector, having such a risk management process is actually a standard requirement. If you don’t you are failing best practice,” says Ralph.

To cut corners, some managers will use industry guidelines such as those provided by the National Institute of Standards & Technology (NIST). The board aren’t necessarily going to know if it’s a template or not; they will assume they’ve been written.

But there are risks to being complacent with regards to developing a strong security posture. Investors are becoming more aware of the issues and national regulators such as the SEC are prioritising cybersecurity as a key initiative in 2016.

RFA is one of only a few certified bodies in the UK under the Cyber Essentials Plus scheme, a UK government-backed initiative to help organisations protect themselves against common cyber attacks.

“We do a cyber assessment, it’s basically a top-level audit of the organisation to identify risks, and issue the client with a certificate. As part of this solution, we have a portal that clients can log on to and do a self-assessment, which contains around 200 questions,” confirms Ralph.

He says that RFA will typically advise clients to conduct one of these audited assessments once a year, during which RFA will go through the responses the client has provided in the self-assessment, check the paperwork, run an intrusion test on the firewall, look at the policies on the firewall and so on.

“A lot of the answers we will already know if they are an existing client of ours. If it is not a client of ours, we would be far more granular with the audit,” concludes Ralph.
“Ultimately, alternative fund managers depend heavily on their third parties and trust them with a lot of sensitive data. Getting those contractual obligations in good order is key,” states Elmer, who adds that they are currently doing risk evaluation exercises with clients so as to best prepare them for the eventuality of an SEC or NFA visit.

“We do this by evidencing the manager’s policies and evidencing the fact that they’ve done due diligence on their service providers, evidencing that they’ve conducted tabletop exercises to prove that they’ve practiced their IRP and that it works, evidencing that their cybersecurity calendar outlines every quarter what training exercise will take place, etc. Showing that audit trail is very important.”

George Ralph is Managing Director of RFA, a leading technology and financial private cloud provider. He makes an important point by stating that any time an asset manager uses outsourced IT vendors for IT development, they will have substantial terms and conditions in place to ensure that their intellectual property rights are protected.

“If, however, you have an internal IT development team, the chances are you won’t have an IPR agreement in place with your staff. These are the sorts of points that we get our clients to think about to properly protect themselves,” says Ralph.

**The human element**

To contain the threat of a cyber attack organisations might think that technology is the fail-safe option. Whilst up-to-date technology is important to an extent, the fact remains that it is the human element that is, and always will be, the biggest threat to suffering a cyber breach. As such, it is incumbent upon fund managers of all shapes and sizes to take seriously the need for ongoing training and education; which is far more cost-effective than buying the latest IDS system, for example.

“One thing we highlight with our clients when we do cybersecurity training is that every single employee is a target,” says Lozada.

“Threat actors are patient and disciplined. They do a lot of reconnaissance. They’ll use LinkedIn to work out who works for who, who reports to who, and they are targeting people at home in the hope that that home compromise can be brought into the office. People are going to get phished on LinkedIn, Gmail, Facebook, etc. We therefore stress to users the need to think about things from an online practice perspective, not just to limit it to the office.”

Hackers are continuously devising new and novel ways to penetrate networks but at the end of the day they just want to get paid. And so it becomes a numbers game. They will look to exploit employees with subtle tactics that are designed to catch them off-guard and trick them, for example, into clicking on a link that downloads ransomware, encrypts data, and demands a Bitcoin payment to unlock it.

“Recently, I received an email from Bank of America.co instead of .com. Even though I don’t have a bank account with them it was, nevertheless, a well-written email made to look like something I should respond to. We’ve actually started to use that email as one of our phishing campaigns,” confirms Mark Coriaty, Senior Vice President Strategy & Partnerships, Eze Castle Integration.

Ralph explains that the top five social engineering techniques are: stealing passwords; pre-texting or ‘friending’ where someone tries to build a relationship by posing as an external service provider; phishing attacks; bating, which tries to tempt people with free goods; and tailgating, where someone will follow an employee into the building after they have swiped their security card.

When asked what the risks are to using social media, Ralph advises managers not to simply ban because it would then drive people to doing more on their mobile devices, but rather to make employees aware of the risks and offer alternatives.

“LinkedIn will allow you to sign up using..."
You have enough to think about when launching a new fund. Don’t add technology to the mix. Let Eze handle IT.

Eze Castle Integration has helped launched more than 1,000 firms worldwide and can help your startup achieve institutional-grade technology from Day One.

Contact us at 0207 071 6802 (UK) or 800 752 1382 (US)
Visit us at www.eci.com
The threat within: Mitigating insider risk

Interview with Mark Coriaty

Mitigating insider risk is one of the biggest challenges that organisations face when it comes to remaining cyber secure.

“One thing we’ve seen a lot of with clients is their need for consulting support,” says Mark Coriaty, Senior Vice President Strategy & Partnerships, Eze Castle Integration. “They don’t necessarily have the biggest IT teams and/or might have been more focused on the engineering side than the cyber side. Consequently, they are spending more time learning about the business, as opposed to just putting a solution in place.

“Cybersecurity comes down to operational and procedural policies as well as employee training, which is by far one of the biggest threats to any firm.”

Many of the reasons for internal breaches come down purely to human error, but on occasion it may be the actions of a rogue employee that lead to data misappropriation.

To limit the impact, fund managers can put in place permission controls as a way to manage their policies and procedures, this might allow them to shut off a USB drive, protect different file sets on the back-end etc.

“It is important for whomever is managing the overall IT infrastructure to ensure that people only have access to data that they need for their day-to-day responsibilities, and block them from accessing data in other parts of the organisation,” says Coriaty, adding that employee training has to be an ongoing process.

“For larger firms who hire new employees regularly, managing the process of training them is crucial to maintaining good security. Most hackers target smaller investment managers not to collect credit card numbers, or investor details, but for extortion purposes using the likes of CryptoLocker to pay ransoms.

“This is where proper training becomes instrumental in teaching employees to recognise what potential threats, such as CryptoLocker, look like. Eze Castle Integration recently launched its Eze Managed Phishing & Cybersecurity Training Service specifically for this purpose - to increase security awareness and change cybersecurity behaviors company-wide. We provide it as part of our managed service when we take on a new client,” explains Coriaty.

Rather than run a phishing exercise all at once, Eze Castle performs it in stages with different groups in an organisation. After the first round of training, Eze Castle’s team will send a report to the client’s COO detailing how many people opened the email. This may be 20 out of 50 people, but in the second wave of training progress starts to be made and perhaps only 10 people open the email as education starts to take effect.

“From a best practice standpoint, we visit the client’s office, produce a WISP with their internal IT team and conduct employee training biannually. This ensures that all documentation is kept up-to-date. With respect to the phishing exercises, we do these on a rolling basis throughout the year. The aim is not to target all employees at once but in batches so that they aren’t aware of it happening, much like a real phishing campaign,” says Coriaty.

Training, and the use of common sense, is often the best remedy to reduce internal breaches.

“We put together black and white lists based on types of websites and social media platforms to let firms understand the risks and allow the COO to use permissions to control what employees are doing on the web,” concludes Coriaty.
your Gmail or Facebook account. Don’t do that. Create a new account. And also control the content that employees post on Twitter, on LinkedIn. Keep it personal and not business specific as that will attract potential cyber criminals,” stresses Ralph.

He says that following blogs is fine “but we advise people not to post comments. “People always say that their views are personal and not those of the organisation they work for but that never gets taken into consideration. If someone posts a response that someone doesn’t agree with, they might bear a grudge with the company that person works for and that could expose them to a potential attack. The key point to remember is that social media is not verified. We can all work for any company we want on social media.”

Dealing with a breach

Given that humans make mistakes, the fact is that organisations should have a plan in place to deal with a breach when it happens, not if it happens.

One way to reduce the scope of a breach is to put limits in place on who can access what data within an organisation. This is especially pertinent to C-level executives. They might want access to everything as the COO, but do they really need to see the marketing department files, or the everyday accounts payable files?

There’s a point to this. If, for example, that same COO fell victim to a CryptoLocker attack, if they did not have permission to see certain data sets then equally the piece of malware would likewise not have access to those data sets.

Marcus Lewis is Director, Technical Sales at Capital Support, a leading managed IT services provider. He says that they use shock tactics when they visit clients.

“We use a mock headline on a newspaper that says they suffered a massive breach and the aim is to elicit the response, ‘We wouldn’t want that to happen!’ Our response is, ‘Okay, let’s reverse engineer the situation. What do you need to have in place before and after to manage a breach?’

“That’s when we talk about putting in place a proper risk and incident response plan, an appropriate Business Continuity plan. Cybersecurity is about how to cope when your data centre goes down, or your telephone network goes down. If there is a malware attack, make sure you have backups in place because you’re only going to lose the most recent data on the network,” says Lewis.

That ability to respond effectively to a breach is precisely what Datto offers to the marketplace. It provides comprehensive backup, recovery and business continuity solutions, which it deploys using the SIRIS 3 data protection platform.

If someone falls victim to a ransomware attack, by using SIRIS 3 clients simply revert to the most up-to-date clean backup of their system, thereby circumventing the threat posed by the ransomware attack.

“The end user would see the ransom note pop up and they would be unable to access their files. It’s at this point that they would get on the phone to their IT vendor who has a partnership in place with us and they would then look at the most recent backup, check it’s clean, and do a full restore.

“This gives clients piece of mind. They know that they have the ability to fully recover from a ransomware attack, or indeed a natural disaster, in a matter of minutes rather than a matter of days or, worse still, not at all,” says Carrie Reber, Vice President of Marketing at Datto.

Hackers play the law of averages. They know that if they send out 1,000 emails there are going to be a certain number of companies that end up paying the ransom.

As Reber recalls: “A hospital in California recently paid USD17,000, and there was a similar case of a university in Canada that paid the ransom because they just didn’t know what to do.

“Clients of ours using the SIRIS solution via their IT service provider have suffered attacks and simply rolled back to the most recent backup and avoided paying the ransomware altogether. It’s a very effective post-breach solution.”

Reber concludes by offering the following words of advice: “Think about preventing an attack but equally as important, think about how to recover from an attack. Make sure you have a knowledgeable IT service provider who can be sure to help you recover quickly, and with minimal disruption.”
Managed Security Services

Capital Support offers a holistic suite of robust security services to meet the needs of the finance sector.

Cyber Secure Protect and Detect
Through intelligent dual layer firewalls and traffic monitoring, Cyber Secure Protect and Detect provides next generation perimeter protection that prevents imminent cyber-attacks from breaching your systems, and allows you to provide appropriate access to staff.

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

Security Risk Management
Security Risk Management provides guidance and support to help you create a security framework that meets regulatory standards. We use ISO 27001:2013 and U.S. SEC standards to help fill gaps in your business security provisions.

Cyber Secure Managed Phishing
Cyber Secure Managed Phishing improves your users' awareness and behavioural response. By delivering planned phishing attacks and providing point-in-time training, the service helps staff protect you from phishing attacks.

For more information on any of our Managed Security services, please get in touch.

PROTECT YOUR BUSINESS

020 7458 1250
info@capitalsupport.com
www.capitalsupport.com

THE MOST TRUSTED & RESPECTED IT PROVIDER
The impending introduction of General Data Protection Regulation ('GDPR') in 2018 is going to affect all organisations in terms of how they protect data. Marcus Lewis, Director, Technical Sales at Capital Support, a leading managed IT services provider, believes that within the funds industry, irrespective of whether it is UK law, EU Law or US law, "managers will comply, but of more concern to them is how they can demonstrate to their investors that their data is secure."

“Our view is that the UK will have to subscribe to EU guidelines, because when organisations are doing business inside and outside the UK, the data protection standards will need to remain the same. The changes that are coming in under GDPR are in line with changes in technology, changes in the way people work, and changes in the way data is stored,” says Lewis.

Lewis believes that UK fund managers should treat data protection in a similar way to cybersecurity guidelines that the SEC have issued to US fund managers. The FCA have yet to produce their own guidelines, so as best practice UK fund managers should broadly adhere to the SEC’s guidelines.

“The same logic applies to data protection under GDPR. Work towards adhering to those guidelines, and wait and see what the UK does. We haven’t left the EU yet and the shortest possible exit will take two years, by which time the EU rules on GDPR will already be out,” says Lewis.

One point that UK fund managers should be mindful of is that the penalties for failing to protect data under GDPR will be more severe than under the UK Data Protection Act. Under the latter regime, companies only face a maximum GBP500K fine. Under GDPR, it is possible that the EU could impose a penalty equivalent to 4 per cent of an organisation’s global revenue.

“The reputation of a fund manager would be seriously impacted. Firstly, would they be able to pay the penalty? And secondly, would they survive the reputational hit to the business? With these events, often it is less about the data breach itself and more about the fact that it happened in the first place,” comments Lewis.

Managers should think about how to spend what IT budget they have available more intelligently.

“What is preferable: good security or a slightly faster laptop? From a productivity perspective it might be better to have the laptop, but from a business perspective it’s better to protect the reputation of the firm by allocating some capital on training and awareness. It’s about thinking how you do business, and how the people and processes are aligned to keep the business secure,” advises Lewis.

He adds that when Capital Support works with start-up managers, the route to becoming cyber secure – and protecting the firm’s sensitive assets – always starts with the basics. This involves setting the right tone from senior management, putting initial rules and processes in place, segregating data, and making sure that everyone is aware of security risks.

“We offer a security risk management service, whereby we walk the client through the potential risks and pitfalls they might face. What we don’t do is dictate what they should do. We simply highlight the risks and empower them to make decisions that are most important to their business at that point,” concludes Lewis.
Intelligent access to cyber security

Europe’s first cyber security ETF

Cyber crime is growing, threatening all governments, companies and individuals as they do more online. In response, the global cyber security industry is estimated to grow from $106 to $170 billion* over the next 5 years.

ETF Securities, together with ISE ETF Ventures, now provides investors with an intelligently designed, efficient and convenient way to invest in leading cyber security companies.

etfsecurities.com/cyber

* Source: Cyber Security Market by Solution - Global Forecast to 2020 published by marketsandmarkets.com

This communication has been issued and approved for the purpose of section 21 of the Financial Services and Markets Act 2000 by ETF Securities (UK) Limited which is authorised and regulated by the United Kingdom Financial Conduct Authority.

The fund discussed in this communication is issued by GO UCITS ETF Solutions Plc (the “Company”). The Company is an open-ended investment company with variable capital having segregated liability between its sub-funds and is organised under the laws of Ireland. The Company is regulated, and has been authorised as a UCITS by the Central Bank of Ireland pursuant to the European Communities (Undertaking for Collective Investment in Transferable Securities) Regulations, 2003 and is structured as an umbrella company with multiple sub-funds.

Investments may go up or down in value and you may lose some or all of the amount invested. Past performance is not necessarily a guide to future performance. The information contained in this communication is neither an offer for sale nor a solicitation of an offer to buy securities nor shall any securities be offered or sold to any person in any jurisdiction in which an offer, solicitation, purchase or sale would be unlawful under the securities law of such jurisdiction. This communication should not be used as the basis for any investment decision. You should consult an independent investment adviser prior to making any investment in order to determine its suitability to your circumstances.

The ETFS ISE Cyber Security GO UCITS ETF (the “Fund”) is not sponsored, promoted, sold or supported in any other manner by International Securities Exchange, LLC (the “Index Provider”) nor does the Index Provider offer any express or implicit guarantee or assurance either with regard to the results of using the ISE Cyber Security® UCITS Index Net Total Return (the “Index”) and/or Index trademark or the Index price at any time or in any other respect. The Index is calculated and published by the Index Provider. The Index Provider uses its best efforts to ensure that the Index is calculated correctly. The Index Provider has no obligation to point out errors in the Index to third parties including, but not limited to, investors and/or financial intermediaries of the Fund. Neither publication of the Index nor the licensing of the Index or Index trademark for the purpose of use in connection with the Fund constitutes a recommendation by the Index Provider to invest capital in the Fund nor does it in any way represent an assurance or opinion of the Index Parties with regard to any investment in the Fund.
When ETF Securities launched the ETFS ISE Cyber Security UCITS ETF (‘ISPY’) in September 2015 it was the first ever cybersecurity ETF in Europe. It was also the latest example of ETF Securities’ commitment to delivering innovative products. ISPY is a smart beta ETF that tracks the ISE Cyber Security UCITS Index Total Net Return using a rules-based methodology developed by ISE ETF Ventures in partnership with ETF Securities. For inclusion in the index, each cybersecurity company must have a minimum USD100million market cap with an average daily turnover of at least USD1million. The ‘smart’ element involves using a growth factor to equally weight the index with a diversified range of global cybersecurity companies across industry sectors. Small-cap and mid-cap companies make up approximately 75 per cent of the index.

“One of the themes that we’ve been working on over the last few years is disruptive technology,” says Rahul Bhushan, Product Specialist at ETF Securities. “We’ve seen strong interest in ISPY since launch. ISE, our index provider, launched a similar product in the US in 2014 which at its peak had assets of USD1.4billion, and we wanted to be the first in Europe to provide similar exposure.”

“In early 2016, volatility that emanated from the global equity market spilled over into the cybersecurity sector, which led the index to post negative performance. We cautioned investors not to fall into the trap of thinking that the cybersecurity sector was weak. Our view is that this sector has significant growth potential,” adds Aneeka Gupta, Equity & Commodities Strategist, ETF Securities. If one looks at the statistics, they support Gupta’s outlook. The number of cybersecurity firms is estimated to grow by 70 per cent between now and 2020 according to PwC research. Also, it is estimated that the cybersecurity sector will grow from USD107 billion to USD170 billion over the next five years.*

“When we present ISPY to clients we want them to think about opportunity in 4 different ways. The first is event-driven capital appreciation. High profile cybersecurity attacks may cause short-term volatility in the markets. The ETF can be an effective vehicle for investors to benefit from the performance of cybersecurity stocks when high profile attacks occur,” explains Bhushan.

The second is long-term capital appreciation. The companies in the index are by and large small- and mid-cap companies with strong growth prospects.

“Third, ISPY offers high-growth diversification of existing investments. The majority of cybersecurity companies held by ISPY are not held by broad-based technology funds. As such ISPY may help investors in broad-based technology funds increase their overall portfolio diversification,” says Bhushan. “Finally, this is a burgeoning sector with high probability of M&A. When there is any offer made on constituents this may lead to a spike in the price and benefit the index. We saw this, for example, when FireEye acquired Mandiant Corp for USD1 billion in January 2014, causing its share price to climb by more than 30 per cent. Also, when Cisco Systems acquired Sourcefire for USD2.5 billion in October 2013, Sourcefire’s share price climbed 28 per cent.”

With cybersecurity now regarded as an integral part of the technology sector, this appears to be a good time for investors to build exposure into their portfolios, and benefit from the potential opportunity that cybersecurity presents.*

*Source: Marketsandmarkets.com, Cyber Security Market By Solution – Global Forecast to 2020
Emerging technology has a tendency to go through a ‘hype cycle’ when investor optimism leads to runaway valuations. The classic reference point is the dot.com bubble at the turn of the century, when tech stocks saw their price to earnings ratios spike above 60 times earnings.

With respect to cybersecurity, although the P/E ratio of stocks at the start of the year was 53 times earnings, it has since come down to 42 times earnings. That is still relatively high, from a valuation perspective, but the signs are that cybersecurity, as a sub-sector, should no longer be viewed as an emerging technology.

“We wanted to figure out where exactly in the hype cycle, produced by Gartner, cybersecurity fits in. We looked at the relative spread of cyber P/E ratios versus technology P/E ratios. What we noticed was that the relative spread peaked in 2014 where it was 65 times earnings. Since then, we’ve seen the relative spread drop nearly half that value to 33 times earnings.

“However, even more interesting in 2016 has been the divergence in net income figures. We have seen net income for cyber stocks in the ISE Cyber Security UCITS Index Total Net Return rise 23 per cent, while net income for technology stocks as a whole has declined 3.5 per cent.

“That confirms to us that the cybersecurity space continues to show strong profitability, with the technology sector at large looking more like a large cap laggard,” comments Aneeka Gupta, Equity & Commodities Strategist, ETF Securities, whose cybersecurity ETF, ETFS ISE Cyber Security GO UCITS ETF (‘ISPY’) tracks the above mentioned index.
Since the index was launched in 2006, it has gained 352 per cent compared to the Nasdaq 100, which is up 135 per cent, whilst the MSCI World Index has gained 28 per cent.

There is no doubt, therefore, that cybersecurity stocks are becoming a valuable component of the technology mix.

“When we look at the reduction in relative spread (to technology stocks) and compare it to Gartner’s hype cycle, we consider cybersecurity to be nearing what is known as the ‘plateau of productivity’. In other words, cybersecurity is no longer a new concept that everyone is getting familiar with but something that is becoming more ingrained and part of the technology ecosystem. Cybersecurity spending, for example, is forecast to rise from USD71 billion in 2015 to USD98 billion in 2018,” adds Gupta.

This is encouraging news. But what are some of the more exciting and innovative companies that are operating in this space? The remainder of this chapter will profile three companies, each of which brings something unique to the table when it comes to helping organisations improve their cybersecurity posture.

**FireEye**

FireEye aims to prevent advanced cyber threats, data breaches and zero-day attacks by using what it calls the FireEye Adaptive Defense approach. The rise of Advanced Persistent Threats (‘APTs’), which work by infiltrating an organisation’s internal network to build a picture of the firm’s activities over a period of months, has been pronounced in recent times.

To combat this, FireEye focuses its efforts on three key areas within its portfolio of products, services, and intelligence: detection, analysis, and response.

“The problem we try to solve is that with all the different breaches and intrusions we’ve seen over the last couple of years, whilst the traditional model of trying to block everything is a good start, it doesn’t mitigate the risk to stopping these breaches becoming egregious and potentially damaging.

“What our portfolio of products, services and intelligence focuses on is to enable organisations to detect intrusions in a timely manner, with a low rate of false positives, before these intrusions go undetected for a period of time. The industry average is five months for a breach to be detected. We allow organisations to detect intrusions within hours and stop them from becoming breaches. This happens when an intrusion persists for months and allows the attacker to collect information within the network,” explains Joshua Goldfarb, Vice President, CTO – Americas at FireEye.

In addition, FireEye provides capabilities for analysis or forensic investigations to help organisations understand what is going on at any given time within their network. The aim is to contain and remediate a threat, or any type of intrusion that is identified, and then eradicate it.

**Signature-based attacks**

Back in the day, firms would use signatures to identify malicious behaviour. But then people started to ask, ‘What if we see something for the first time, even though there’s no signature for it?’

Think about airport security as an analogy. One day, somebody tried to smuggle liquid explosives onto an aircraft and the response was to ban liquids. Then somebody tried to detonate a device in their shoe so the response was to ask people to take off their shoes at the security gate.

These are all examples of signature-based detection. You’re looking for something that you’ve seen in the past.

The above logic is flawed. It is an example of what academics would refer to as a Syllogistic Barbarism, a form of reasoning that works by using a major premise, a minor premise to produce a false conclusion i.e. All carrots are orange. Some cats are orange. Therefore, some cats are carrots.

Many people wear shoes and have no intention of blowing up an aircraft. Similarly,
RANSOMWARE attacks in Q1 of 2016 increased tenfold from the entire previous year, costing victims more than $200 MILLION.

Thanks to their partnership with Datto, ACE IT Solutions customers didn’t have to pay a penny.
How to recover from a ransomware attack

Interview with Warren Finkel & Carrie Reber

Companies across all sectors are increasingly dealing with ransomware attacks as cyber criminals attempt to extort money by encrypting files and effectively holding data hostage. There are endless versions of ransomware but some of the more well known include: CryptoLocker; CryptoWall; TeslaCrypt, and CTB-Locker.

To underscore the scale of the problem, the FBI reported that in the first quarter of 2016, ransomware costs in the US totalled USD209 million. For the whole of 2015, the figure was USD24 million.*

The McAfee Labs Threats Report 2015 found that between Q4 2014 and Q1 2015, the number of ransomware attacks increased from 260K to 725K.

To combat this threat, fund managers need to have up-to-date antivirus software and a robust business continuity and disaster recovery plan. ACE IT Solutions, a leading IT group and provider of managed services and cybersecurity solutions, has partnered with Datto to give clients an effective solution to circumventing ransomware attacks. Datto provides comprehensive backup, recovery and business continuity solutions, which it deploys using the SIRIS 3 data protection platform.

“The way ransomware works, someone will log in and discover that their files have been encrypted. They’ll see a message demanding payment to unencrypt the data. The most common route is via a phishing email that looks authentic and tricks the user into clicking on a link. We had one example of a client who thought they had been sent an invoice. An employee opened up the invoice and inadvertently downloaded the ransomware.

“The scary thing with ransomware is that it doesn’t just infect one person’s PC, it can infiltrate the entire network, including servers. Unless you have the encryption key you won’t be able to unencrypt the files,” explains Carrie Reber, Vice President of Marketing at Datto.

To neuter these attacks, the SIRIS 3 platform automatically takes backups of files at whatever interval a client wants.

ACE IT Solutions will run constant backups on behalf of its clients, alleviating the stress on IT teams. One important aspect of the SIRIS platform is Backup Insights, a tool that allows users to examine backup files.

“The reason this is useful is that some forms of ransomware sit dormant on the system before they reveal themselves. The hope is that this will allow the hacker to get into your backup files. With Datto, partners like ACE IT Solutions can examine their clients’ backup files and determine whether the most recent backup has also been infected.

“If it has, ACE IT Solutions will go back to the one before that and so on, until it locates the most recent clean backup, which is then used for the full restore,” says Reber.

This completely circumvents the ransom demand and renders the attack obsolete.

“You definitely need perimeter defense systems like antivirus software, and you need to maintain a well-managed IT infrastructure with proper controls and user permissions, but even doing all of these things there’s always going to be a moment of human error, or a social engineering attack, that leads to something getting through. And that’s where a reliable IT partner with a reliable backup solution like Datto comes into play; we step in once the breach has happened and allow businesses to recover without paying a penny to hackers,” concludes Warren Finkel, Managing Partner of ACE IT Solutions.

it doesn’t help you next time you are hacked as the threat actor is going to use a different method to try and get around one’s signature-based detection.

“We in the security field realised that a new approach was needed, which we call detonation. When we have a file, the best way to learn what it does is to run it in a controlled environment – a cage – where it can’t do any harm to the organisation. By analysing it, we can determine that if it were to get out of the cage, whether it would be benign or malicious.

“What we are now beginning to realise is that attackers are shifting to using stolen credentials and passwords. To detect that particular layer, we need to use analytics to identify departures from expected behaviour at the user level and the system level. This is still an emerging field. We’re evolving our detection capabilities and focusing heavily in this field of analytics to keep pace with the attackers,” explains Goldfarb.

Goldfarb thinks there are two root causes of large breaches. The first is something he refers to as ‘alert fatigue’. This is where organisations have a series of detection systems deployed not specifically tailored for their risk profile, and they receive thousands of alerts, the vast majority of which are false positives. This noise makes it very difficult to pick out the signals that imply an actual intrusion is taking place.

“All of our detection technology is designed to produce a fewer number of high quality signals and very few false positives,” says Goldfarb.

The second cause is lack of context. Even if you’ve removed the alert fatigue problem, it is hard to make a decision on whether something is good, bad or indifferent until you enrich that alert with the necessary context. This comes from using different data sources, different intelligence and other types of supporting evidence to make an informed decision.

“Those two together are the main reason for why we see so many attacks today. An attacker gets in, hides in the noise, and if someone does find the alert, they have a hard time enriching it with the necessary context to make a correct decision on whether an intrusion has happened,” says Goldfarb.

“An attacker gets in, hides in the noise, and if someone does find the alert, they have a hard time enriching it with the necessary context to make a correct decision on whether an intrusion has happened.”

Joshua Goldfarb, FireEye

Digital Shadows

London-based Digital Shadows was established by Alastair Paterson and James Chappell in 2011. Whilst FireEye focus on the threats coming in to one’s network, Digital Shadows helps assess external threats, providing its clients with what it refers to as cyber situational awareness.

In short, Digital Shadows monitors the online digital footprint of organisations from a security standpoint. It aims to prevent, detect and help contain cyber-related incidents by analysing the organisation through an “attacker’s eye view”.

“Having a digital footprint is a good thing. When a company interacts with the Internet the trail that it leaves behind it is, for the most part, good; interacting with customers, conducting research, building insights. There are net benefits to most organisations. But there is some part of our online experience where information is relevant from a security and risk perspective. Rather than call that a digital footprint, we call it a digital shadow,” explains James Chappell, CTO and Co-Founder of Digital Shadows.

There are three main elements of the digital shadow:

• Data loss – confidential documents that end up outside of an organisation’s network;

• Weaknesses in the defenses of an organisation – the sort of clues that an attacker would use to focus their attacks;

• Understanding the threats by monitoring the Internet.

Digital Shadows monitors all three of the above, alerting clients whenever it spots something untoward, to mitigate the effects.
PROTECT YOUR ASSETS

FOR ASSET OWNERS AND THEIR GATEKEEPERS, CYBERSECURITY HAS BECOME A TOP OPERATIONAL DUE DILIGENCE PRIORITY.

Evaluate the cybersecurity environment and derived cyber risk at asset managers in your portfolio.

Leverage Castle Hall’s decade of operational due diligence experience, cybersecurity expertise and award-winning due diligence platform, DiligenceProfessional™

- Detailed CyberSecurityDiligence of individual managers – or a full portfolio
- Ongoing CyberSecurityDiligence monitoring
- Reporting through DiligenceProfessional™ web-based portal

Contact us to learn more about our innovative Cybersecurity due diligence services for institutional and private investors.

cybersecurity@castlehallalternatives.com
+1 450 465 8880

www.cybersecuritydiligence.com
Cybersecurity has rapidly become one of the most discussed issues in the alternative asset management industry. Regulators have provided multiple warnings around the need for investment managers to protect their businesses from cybersecurity risks. In response, both industry groups and tech consultants have published advice to help asset managers implement cybersecurity protections.

On the other side of the industry, asset owners are now acutely aware of their governance, risk and compliance obligations to evaluate the cybersecurity preparedness of external asset managers within their operational due diligence programmes. However, investors must bridge the gap between highly technical subject matter and more practical guidance as to how to approach cybersecurity during a real world operational diligence review. Earlier this year, Castle Hall Alternatives published Evaluating an Asset Manager’s Cybersecurity Environment – A guide for the operational due diligence practitioner, a white paper discussing cybersecurity in the context of operational due diligence.

10 key risk categories
The alternative industry comprises many thousand asset managers, varying enormously by assets under management, headcount, and overall quality of operational infrastructure. To provide a standardised evaluation framework across such a diverse landscape, Castle Hall has identified 10 cybersecurity diligence risk categories to support investor oversight and diligence.

Data classification: All data that the manager handles should be assigned a formal sensitivity level and data category. A well-structured cybersecurity framework maps the flow of data through creation, access, processing and destruction points on both internal and third party infrastructure.

User access: Managers should limit user access to appropriate data, according to least-privilege and need-to-know principles. Access to the manager’s data and IT resources should be provided through roles that map job functions to data sensitivity levels and data categories.

Data, network and hardware security: Managers need to follow a “defense in depth”, layered approach, where multiple detective, preventive, corrective and recovery security controls are deployed between a potential attacker and the manager’s data. Security controls always have to travel with the data.

Change management: Managers must maintain an inventory of all their IT assets, follow standardised processes and procedures, and understand the implications of changes to the IT infrastructure before they are made.

Personnel: Managers should have a dedicated Information Security resource (individual or department) with the authorisation and means to assess, monitor and defend all of the manager’s data and information systems.

Vulnerability and patch management: The manager needs to proactively evaluate vulnerabilities and ensure that security patches are applied on a timely basis.

Incident response: Regardless of the nature of the incident, a timely response is essential. Having a tested plan helps ensure efficient and effective responses that limit the damage to a manager’s data and reputation.

Security awareness and training: Awareness of the importance of cybersecurity, familiarity with policies and procedures, and reinforcement of proper practices are essential for understanding and avoiding cybersecurity risks.
He goes on to explain that the types of 'needles' that it looks for might include: assets showing up in places they shouldn't be (i.e. criminal forums); monitoring for vulnerabilities (i.e. passwords and network credentials being leaked out); attack strategies that might be useful to attackers, etc.

"Every day, an organisation's digital footprint might consist of many tens of thousands of different components. What we do is to reduce that footprint to the 10 most pertinent things that the organisation should be aware of to maintain good security."

"We can also give clients forecasts of what threats might be coming next to help them align their defenses," adds Chappell.

Darktrace

Darktrace was founded in Cambridge, UK, in 2013 by mathematicians and machine learning specialists from the University of Cambridge, together with world-leading intelligence experts from MI5 and GCHQ, to bring transformative technology to the challenge of cybersecurity.

Whilst FireEye and Digital Shadows provide highly effective solutions to protect against internal and external threats to one's network, Darktrace provides something altogether different. It provides an active prevention and response capability that is built on a highly sophisticated system framework that utilises the latest in machine learning capabilities.

The result is something that the Darktrace refers to as 'Enterprise Immune System technology' - the only cyber defense technology that is capable of detecting anomalous behaviors within large and complex environments, without any prior knowledge of what it is looking for.

In years past, people would try to prevent attacks from happening at all but the simple fact is this is impossible. Every organisation...
Are You at Risk for a Cyber Breach?

PREPARE  RESPOND  RECOVER

Cybersecurity is a vital part of the business fabric. As technology continues to advance, so does the potential for increased cyber threats. Our Cybersecurity, Compliance, and Forensic experts around the globe will help your business improve its security posture and develop plans to prepare for, respond to, and recover from a compromise.

www.duffandphelps.com

Contacts:
Jason Elmer
Cybersecurity Services
+1 212 871 6366
jason.elmer@duffandphelps.com

Brian Lozada, CISSP
Cybersecurity Services
+1 212 871 9755
brian.lozada@duffandphelps.com

Duff & Phelps is the premier global valuation and corporate finance advisor with expertise in complex valuation, cybersecurity, dispute and legal management consulting, M&A, restructuring, and compliance and regulatory consulting. The firm’s more than 2,000 employees serve a diverse range of clients from offices around the world. For more information, visit www.duffandphelps.com.
Cyber attacks: Prepare, respond and recover
Interview with Jason Elmer & Brian Lozada

Asset managers are increasingly focused on cybersecurity best practices not only to stay in line with regulatory expectations but also to be viewed in a positive light by investors.

According to Jason Elmer, who heads up Duff & Phelps’ Cybersecurity practice with fellow Managing Director, Brian Lozada, “When I attend industry conferences, even those not specifically focused on cybersecurity, and the audience votes on what their biggest concern is for 2016, cybersecurity comes out on top; just about even with the challenge of asset raising.”

To meet that challenge, Duff & Phelps launched a dedicated cybersecurity services solution to help organisations identify network vulnerabilities and implement best practices to limit the chances of a breach.

The mantra that Elmer and Lozada like to use to summarise the Duff & Phelps offering is “Prepare for, respond to, and recover from”.

“From a preparation perspective,” says Lozada, “we align ourselves to our clients’ business workflow. We want to understand what their business is, what their sensitive assets are, and we then put a lifecycle around those sensitive assets.

“Once we have a good understanding of that we help align our clients’ security efforts to that lifecycle so that if and when a breach takes place, they are able to respond properly with regards to protecting that sensitive data.”

In addition to providing clients with the Written Information Security Policy (WISP) and Incident Response Plan (IRP), guiding them on how to respond to regulators, and performing due diligence on their third party providers, Duff & Phelps will also go in and train clients on best practices.

“That comes in the form of introducing the policies and procedures to the organisation, as well as talking through the various ways that employees can avoid being compromised both in the office and out of the office,” says Elmer.

He continues: “When we track the lifecycle of data, we even track internal users with access to that data, as well as third parties. When we develop the IRP, we take all of those parties into consideration.

“Indeed, we like to include external legal counsel as part of the incident response, the investor relations team - basically anyone that is involved with the data that has been breached we involve in the incident response plan. This is not only about protecting clients’ data; it’s also about protecting their brand.”

The IRP is vital in any recovery effort and surprising as it may sound, there are still plenty of fund managers who don’t have one in place.

In the event that a serious breach occurs, Duff & Phelps has its own cybersecurity forensics response team. The team will make a forensic copy of the client’s hard drive that was compromised, conduct an investigation on it and then turn it over to relevant bodies such as law enforcement agencies, and the client’s litigation team.

“When clients use us to write their WISP and IRP we include Duff & Phelps as the body that will go in there and do a forensic investigation,” says Lozada. “And even for those clients that don’t subscribe to that service, we are very happy to help them source a forensic partner, vet them, and include them in the client’s IRP and tabletop exercises. Our clients increasingly understand that they need to take a proactive stance to dealing with cybersecurity across their firm.”

Jason Elmer, Managing Director, Duff & Phelps’ Cybersecurity practice
Brian Lozada, Managing Director, Duff & Phelps’ Cybersecurity practice
will be breached at some point. Therefore, it
one knows this, how can they possibly figure
out when they’ve been attacked if they don’t
know what they are looking for?

Threat actors are using novel techniques
and ways of getting inside networks. At
the same time, businesses are working
with smaller resources and budgets. Yet
they need an effective way to police the
landscape and figure out if they’ve been
compromised.

“Imagine you are a security guard
at a train station and you’re trying to
spot someone suspicious. It’s not easy.
Likewise, you can hire people to comb your
organisation to look for potentially suspicious
activity. The problem is that an organisation’s
network is extraordinarily complicated.
It’s got millions of pieces of data moving
around, and it is almost impossible to police
manually. You need technology that can act
as a set of digital eyes that keeps a constant
eye on the network and watch for any bad
things happening.

“This is what we are trying to do at
Darktrace. Technology has made huge
advances in recent times, especially with
respect to machine learning, such that
we can now make systems that perform
that sentinel function within the network,”
explains Andrew Tsonchev, Cyber Security
Specialist at Darktrace.

In effect, what Darktrace has produced
is a system that fits inside one’s network
where it performs the digital role of the train
station security guard, constantly monitoring
data flows every millisecond.

As mentioned above, FireEye looks for
malicious files, programmes, that come into
the network and stops them from doing
damage. They look at everything – good or
bad – coming into the network and decide
whether it is a threat or not.

“We don’t look at all the files and
programmes coming in, we look at the
symptoms,” says Tsonchev. “If a suspicious
file enters the network and infects it, we look
at changes to the behaviour of computers
and people within the organisation to infer
that they’ve been infected.”

The implications to this are huge. What
Darktrace is doing is to turn the endless
arms race that exists within cybersecurity
on its head – it makes no attempt to stop
the attacks from happening, as the nature
of attacks continuously changes. Rather, the
Enterprise Immune System technology works
just like that of the human body. It doesn’t
react to everything that enters it. Instead, it
waits to see what the symptoms are and
responds accordingly.

“That is how we developed the system;
not to stop something coming in but to look
for changes in behaviour that triggers an
immune response. Organisations need to
know what is going on inside their network.
It’s only by knowing what’s normal that they
can detect when things have changed and
figure out that they’ve been compromised,”
says Tsonchev.

He adds: “All we do is look for the
symptoms of a potential breach within a
network. And that totally changes things.
Given the increased sophistication and
novelty of attacks, defense is no longer just
a game of preventing attacks from getting in,
but one of early detection and response to
threats already inside.”

One might ask how the system is able to
determine what constitutes a real threat and
a false threat. Indeed, this is the Holy Grail.
As it uses machine learning, Darktrace’s
solution learns about its ‘self’ over time such
that it builds intuition as to what looks like
normal activity within a network, and what
might constitute abnormal activity.

“The key is to look for the right things. In
machine learning we refer to this as ‘feature
selection’. We continually compare every
device to every other device and build up a
rich comparison of activity between all the
computers in the network that allows us to
look for really interesting changes, and avoid
all the mundane deviations that occur in
organisations every day.

“We’ve effectively built a super vigilant
digital security guard that can look at a
million computers simultaneously and work
out that it has a bad feeling about one
of them because the way it is behaving
unusually,” concludes Tsonchev.

There are incredible innovations taking
place in the cybersecurity sector. And as
the sector continues to grow and evolve,
there will be more companies such as those
profiled above over the coming years. It is, in
short, one of the most fascinating areas of
the technology space.