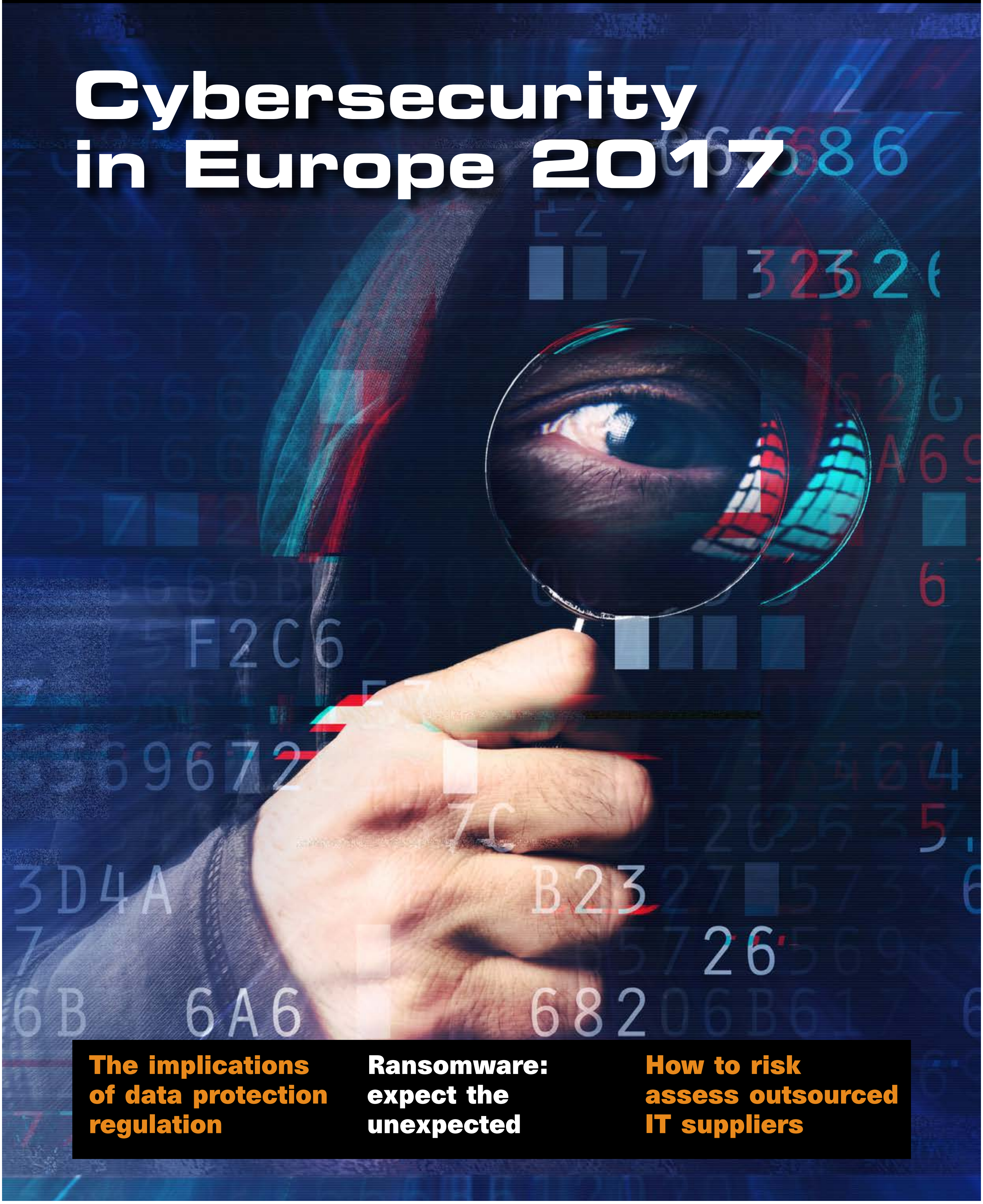
hedgeweek special report
www.hedgeweek.com
July 2017

Cybersecurity in Europe 2017



The implications of data protection regulation

Ransomware: expect the unexpected

How to risk assess outsourced IT suppliers

In this issue…

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: Mary Gopalan, mary.gopalan@globalfundmedia.com
Graphic Design: Siobhan Brownlow, siobhan.brownlow@globalfundmedia.com
Sales Managers: Simon Broch, simon.broch@globalfundmedia.com;
Malcolm Dunn, malcolm.dunn@globalfundmedia.com;
Sales Manager, Private Equity Wire: Christine Gill, christine.gill@globalfundmedia.com;
Sales Manager, Property Funds World: Matthew White, matthew.white@globalfundmedia.com
Marketing Administrator: Marion Fullerton, marion.fullerton@globalfundmedia.com
Head of Events: Katie Gopal, katie.gopal@globalfundmedia.com
Chief Operating Officer: Oliver Bradley, oliver.bradley@globalfundmedia.com
Chairman & Publisher: Sunil Gopalan, sunil.gopalan@globalfundmedia.com
Photographs: iStock Photo; various
Published by: GFM Ltd, Floor One, Liberation Station, St Helier, Jersey JE2 3AS, Channel Islands
Tel: +44 (0)1534 719780 **Website:** www.globalfundmedia.com

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.

hedge**week**

The implications of GDPR on cybersecurity

By James Williams

Next year sees the introduction of a comprehensive piece of European regulation that will overtly change the way that organisations handle, store and protect data. Known as the EU General Data Protection Regulation (GDPR), it arguably represents the most significant change in global privacy law in 20 years and will require fund managers to shore up their cybersecurity processes and procedures to avoid facing financial penalties.

GDPR is due to be implemented in May 2018 and places important new obligations on any business that handles the data of individuals living in the EU, independent of where the business is located. It is this 'extraterritoriality' of GDPR that global fund managers really need to be aware of. Anyone marketing their fund(s) into Europe and who has existing EU investors will be required to comply with GDPR or face the consequences.

"During a recent trip to New York, what came up frequently was discussions over GDPR. Most were not aware of exactly what it is," comments George Ralph, Managing Director of RFA, a leading provider of IT solutions and advisory services to the financial services industry.

At the heart of GDPR is data protection. As such, it overlaps significantly with respect to managers maintaining a strong cyber posture to protect fund data, especially personally identifiable information on their investors. Both fund managers and their counterparties will need to ensure that all proper measures are being taken to protect that data, so that in the event of a cyber attack, they have a proper incident response plan in place to respond swiftly and mitigate the loss of said data.

"The big investment banks have been working through GDPR programmes for the last two years or more but other institutions

– both traditional and alternative fund managers – may not have been focusing on it. The one-year-to-compliance deadline and increased media coverage of GDPR has led to focusing more on it," says Rohan Massey, Partner at Ropes & Gray, where he leads the firm's privacy and data security practice in Europe.

"We are receiving more calls from clients asking what they need to do to comply, and how do they get there. No organisation wants to be subject to a financial penalty, which could be as high as 4 per cent of one's annual turnover. Under the old regime (UK Data Protection Act of 1998) the risk was that if an entity breached its compliance obligations it alone got issued with a fine. Under the new regime, the power to level the fine extends to a much wider pool of economically linked undertakings. It is a sea change in the regulatory power that can be enforced."

Anyone who is a data processor – i.e. a fund administrator, a cloud provider – and not the data controller, is now partly liable for the controller's misuse of data. That will be the same for anyone who hosts CRM systems on behalf of the manager, risk consultants, etc.

Under GDPR, there are requirements for firms to have appropriate technical and organisational security measures. As Massey explains, there is a greater burden of documentary evidence on organisations "to show that they've been through a well thought-out process in assessment of their obligations relating to personal data, the types of data they hold, the sensitivity of that data and the volume of that data."

Not that a personal data breach will automatically result in the maximum penalty being levied; this is only likely to happen in the most egregious circumstances where a systemic failure to protect personal data has occurred.

"If a personal data breach occurs, it may mean that the regulator looks at how you've responded and decides you haven't done enough. If you can evidence that you did everything possible to mitigate the impact of the breach, you are likely to reduce the level of any penalty issued," adds Massey.

This is something that Ralph reaffirms: "Most of the examples I've seen and heard about under existing data protection regulation are that if you report a breach and tell the regulator what you are doing, and what steps you are taking to stop it from happening again, often they won't fine you. That said, there are a lot of things that the regulators are expecting firms to do under GDPR, such as the right for people to be forgotten. This poses some challenges: for example, how does a company keep track of data elements that have that person's name included?"

"We are receiving more calls from clients asking what they need to do to comply, and how do they get there. No organisation wants to be subject to a financial penalty, which could be as high as 4 per cent of one's annual turnover."

Rohan Massey, Ropes & Gray

Chris Eaton is Senior Manager with KPMG (Bermuda) and the KPMG Islands Group Cyber Security Lead. Earlier this year, KPMG partnered with AIMA and the Managed Funds Association to determine how managers are responding to technology. The survey found that 60 per cent of managers are thinking first and foremost about data security.

Eaton believes that the impact of GDPR could have tremendous financial implications.

"Those organisations who fall within the scope of GDPR will face a potential fine of 4 per cent of global revenue. Therefore, managers will need to treat personally identifiable information carefully and have proper policies and procedures in place to protect it. I think GDPR will broadly raise the benchmark of the quality of cybersecurity controls because of the impact that this regulation could have on an organisation if they get it wrong," suggests Eaton.

If fund managers weren't already working hard to determine what their most sensitive data is, and ensuring that it is properly protected, they certainly will be as the GDPR deadline ticks down. Aside from any financial

▶ 6

What does a sound cyber strategy look like?

By George Ralph

Cybersecurity has never been as important as it is today. Cyber attacks are becoming ever more ambitious and overt. The two big recent malware attacks, Petya and WannaCry both used phishing attacks to spread malware through networks, with Petya in particular, engaging sophisticated, multi-pronged methods which renders the user's computer inoperable, but also provides the hackers with full access to the usernames and passwords stolen from the computer.

The Cyber Security Breaches Survey 2017, published by the Department for Culture, Media and Sport and undertaken by Ipsos Mori stated some frightening figures about the preparedness of businesses to deal with these sustained and frequent attacks. Whilst 74% of the 1500+ businesses surveyed said that cyber security is a very high priority for their senior management, and 67% have spent money on cyber security in some shape or form in the past year, only 33% have a formal policy that covers cybersecurity risks. In addition, only 11% have a cyber security incident management plan in place.

I believe firms need to take a systematic approach to cybersecurity, covering three main elements. These are policy and procedures, technology, and education and training. Firstly, firms need documented policies and procedures in place to safeguard business data, systems and networks and to meet regulatory compliance mandates. The cyber incident response plan identifies the key systems, processes and personnel involved, and documents how the firm will go about preparing for an incident, detecting one, most importantly containing an incident, recovering from it and how the firm will undertake post-incident analysis.

George Ralph, Managing Director of RFA

The business continuity plan outlines the critical business processes and IT systems, and the recovery procedures and timescales. Finally, the cybersecurity framework details the user training the firm will undertake, the physical security measures they will put in place, how internal audits will happen, how risks will be identified and classified and how the supply chain will be de-risked.

The next step, getting the technology right, the hardware, software and systems, that protect every layer of data, is also more complex than it seems. A robust cybersecurity strategy should be multi-layered, and include email, mobile devices and other endpoints, web traffic and the network. Firms should also take into account data governance, and data should be encrypted, the physical environment should be secure, access should be managed closely, and firms should run regular penetration testing and vulnerability scanning across the technology estate.

The final component to the framework is to educate employees about cybersecurity, and provide effective training to help them identify malicious behaviour and to act accordingly to avoid or mitigate the risks.

One way of doing this is by regularly and without warning, testing users with simulated email, voice and SMS phishing attacks, personalised landing pages, attachments and spoof domains in order to highlight risks and employee weaknesses. When employees fall victim to these attacks they can be given immediate feedback and a refresher on spotting the red flags.

With the threat of attack becoming increasingly more prevalent, it's not enough to do one of the components without the others. Precisely why a thorough and systematic approach is needed. ■

4 ▶ fines they could face in the event of a breach, of far greater material import would be the reputational impact.

"You could face a regulatory administrative penalty on one side, and a class action brought about by individuals – i.e. fund investors – on the other. So GDPR is a big deal, and becomes a central tenet of data management best practice in terms of ensuring the safety of sensitive data," states Massey.

To illustrate the 'teeth' of this new regulation, consider the fact that when the Talk Talk cyber breach occurred in the UK in October 2015, affecting nearly 157,000 customers, they were fined a record GBP400,000 by the Information Commissioner's Office (ICO). This was just shy of the maximum GBP500,000 fine.

Under GDPR, if that attack happened again, they would face a potential penalty of EUR17 million.

There will be a two-tier approach to imposing penalties. The first tier relates to the data controllers. They are the ultimate custodians of their funds' data, and as such they will be subject to EUR20 million or 4 per cent of annual turnover – whichever is greater.

Article 5 of the regulation sets out basic rules on personal data processing, which apply to data controllers. One of those rules requires data controllers to ensure that personal data is "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures".

The second tier relates to the data processors – the fund manager's counterparties such as their fund administrator. In the event of a serious breach, they would be subject to a penalty of up to EUR10 million or 2 per cent of annual turnover.

Data processors will be subject to Article 32, which requires them to "implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk" of their personal data processing.

"It may be that the regulator does not consider a 4 per cent fine to be appropriate in all cases but that's not to say they wouldn't do so in the most extreme cases. While data processors need to be compliant, there's an obligation on the data controller to put in place contractual arrangements stating that all third parties will be compliant with their GDPR obligations. Regardless of whether it's a niche vendor or a large vendor, their obligations are the same," confirms Massey.

"I think GDPR will broadly raise the benchmark of the quality of cybersecurity controls because of the impact that this regulation could have on an organisation if they get it wrong."

Chris Eaton, KPMG

In many respects, with the cyber threat landscape fast evolving, regulations such as GDPR could be considered a positive development. It is at least forcing firms to pay close attention to data security and data management, which at the same time should make it harder for serious breaches to occur.

As the scale and sophistication of attacks grow, fund managers have to remain vigilant and try to put in place sufficient processes and policies to best protect their businesses and remain in compliance with GDPR. Ultimately, cybersecurity and GDPR are one and the same: the common denominator is data management.

"Fund managers need really good cybersecurity frameworks in terms of end-point protection – antivirus, malware tools, firewalls – and have to be careful as to the types of data that employees have permission to access," says Ralph, confirming that RFA has recently been certified by GCHQ to do GAP analysis on GDPR.

"It was an extension of our cybersecurity certification. We are fully certified as part of the IASME governance standard, which demonstrates that we have a robust governance system and can adequately protect personal data belonging to our customers," concludes Ralph. ■

How to respond to increasingly targeted phishing attacks

Interview with Dean Hill & Stephen Banda

According to the PhishMe 2016 Q3 Malware Review, the proportion of phishing emails containing ransomware grew to 97.25 per cent in Q3 last year. This is a threat that is becoming more sophisticated, and more targeted. Not only that, but the frequency of attacks is at an all-time high.

"As people become better aware of what a phishing attack is, so the sophistication of attacks targeting individuals and organisations becomes greater," says Dean Hill, Executive Director, Eze Castle Integration.

This is also being driven by continued investments in technology, making it harder for hackers to breach organisations. There is, in effect, an arms race between organisations and hackers, each trying to stay one step ahead of the other.

Stephen Banda is Senior Product Manager at Eze Castle Integration. Discussing the more targeted nature of phishing attacks, he says: "They are doing a really good job of mimicking an email that might genuinely have come from the CEO. It's difficult for the recipient to discern this unless they really take care to look at the email signature – is there a 1 being used instead of an l, for example, in the person's email name?"

To help firms deal with the ongoing phishing threat, Eze Castle Integration provides an effective solution which it refers to as Eze Managed Phishing & Training. These are basically phishing simulations designed to test employees' susceptibility to phishing.

"We will send emails to clients that look very similar to their day-to-day works emails. We have a huge library of phishing campaigns and we have the ability to customise them based on input from our clients," confirms Banda.

Dean Hill, Executive Director, Eze Castle Integration

Stephen Banda, Senior Product Manager at Eze Castle Integration

In those emails, Eze Castle Integration will ask the recipient to click a link, download an attachment, or fill out log in credentials. Whatever the prompt might be, the aim is to trick them into falling for it. The minute they click on a link, for example, they've failed the exercise.

"At that point they are presented with a learning page, which tells them it was a simulated phishing test and advises them on things to look out for in future, depending on the nature of the email," says Banda.

This managed phishing service is proving invaluable to organisations as they look to develop internal best practices. The better trained staff are, the more likely they will respond to a phishing attack the right way, escalating it to their COO, or to their outsourced IT vendor.

"For each of the Eze Managed Phishing reports we produce, executives get a firm-wide view on how their employees are doing, what the overall level of awareness is, and the extent to which they are improving over time.

"We also have an online training service that goes through some of the key concepts from a cybersecurity awareness standpoint, with an assessment at the end. This too can be tracked by the client," explains Banda.

Ultimately, concludes Hill, every incident response plan should have clear instructions on how to report a phishing email:

"What does it look? When did it happen? What were the contents of the email? Then, there needs to be a proper notification process within the firm – who do you go to when you've identified one of these emails? There has to be a verification path to determine what a potential phishing attack looks like." ■

Insights on the evolving cyber threat landscape

By James Williams

Business has changed markedly over the last few years thanks to the rise and sophistication of digital technologies. As asset managers have evolved to become more automated and utilise a plethora of solutions to manage data, they have unavoidably become more vulnerable to serious cyber attacks. The simple fact is, cyber criminals have an exponentially higher number of attack surfaces to utilise, from cloud computing systems to mobile devices and the Internet of Things.

"What was once a limited attack surface not extending beyond an organisation's firewall has become practically unmanageable," says Jay Kaplan, CEO and co-founder of Synack. "Companies need to take a proactive approach to securing anything that reaches inside the walls of their organisation as any digital device could cause a complete compromise of the integrity of that organisation's data."

Synack is the first hacker-powered intelligence platform and recently announced it had raised USD21.25 million in a Series C round of funding led by Microsoft Ventures. Leveraging a global crowdsourced network of ethical 'white hat' hackers, Synack's platform delivers an offensive approach to defence for organisations, and works with some of some of the largest Fortune 500 companies, hedge fund groups, as well as various branches and agencies of the US Government.

"We started the company four years ago having previously spent four years at the NSA supporting the US intelligence community. That gave us a unique perspective on the cyber landscape and opened our eyes to just how pervasive the problem is – something everyone is starting to realise now. With Synack, we wanted to change an organisation's ability to better understand what they look like in the eyes of an adversary trying to break into them.

"The idea is to mimic what the attackers are doing maliciously, by utilising our highly vetted ethical hackers, to probe and test a technology footprint proactively. This provides prioritised insights so that when someone does try to break into an organisation, it becomes so difficult that they decide it's not worth pursuing," explains Kaplan.

Synack currently has 500 researchers on the platform located in over 50 countries. They are referred to as the Synack Red Team or SRT for short.

"Many existing solutions that attempt to discover vulnerabilities have become highly commoditised. We recruit a global network of white hat hackers and when they successfully find a vulnerability with a client, we remunerate them. In addition, we have a process where we do verification of the client's attempted remediation. The client might believe they've patched a vulnerability but many times there is a way to circumvent that countermeasure, something we are able to discover immediately," says Kaplan.

Rather than being reactive to cyber attacks, organisations are able to work with Synack, and others, to employ ethical hacking strategies that expose vulnerabilities, and address them, before the bad guys come along.

Viktor Tadijanovic is Founding Member and CTO of Abacus Group. Firms like Abacus are responsible for managing all its clients' technology, from an operational standpoint. Although they can't prevent breaches, per se, IT partners can share data-rich reports with clients to highlight if, for example, a disgruntled employee is stealing or deliberating leaking sensitive data.

"An example is file access privileges. Who's got access to which directories? What changes were made? When were those files accessed? We give clients these reports to review and to identify potential red flags. Then they can come back to us and say, 'We think we've seen something suspicious, can you go into this in a little more detail?' We have all the data logs to do this, and potentially identify a rogue employee who is accessing information and appropriating it before they leave," explains Tadijanovic.

"What was once a limited attack surface not extending beyond an organisation's firewall has become practically unmanageable."

Jay Kaplan, Synack

The recent high-profile WannaCry and NotPetya ransomware attacks are symptomatic of how just how serious cybercrime has become, affecting nations and critical infrastructure with massive consequences. As serious as these attacks are, hedge fund managers need to remain pragmatic and do their best to 'right size' the perceived risks to their organisation.

Craig Balding is the founder of Resilient Security, a London-based firm that provides a range of cyber advisory services to global corporations. Prior to this, Balding was Managing Director within Global Information Security at Barclays PLC.

He acknowledges that for hedge funds, the challenge is trying to put a number on cyber risk.

"They will have governance and risk management frameworks in place but many struggle to determine what their cyber risk exposure is, and also what their appetite is. You can't be perfect, or strive to be. I do think being able to price someone's cyber risk is the elephant in the room," says Balding.

"So much of it is about recognising where you are," states Eldon Sprickerhoff, founder and chief security strategist for the cybersecurity services company eSentire Inc. "It requires sitting down and making pragmatic decisions: what are you allowed to do (as the CTO) and what can you afford to do? What makes the most sense for your firm?

"What are the areas that can be acted upon right away to show the board you are

▶ 12

Cybersecurity challenges for investment managers

Interview with John Araneo & Vinod Paul

The Cybersecurity phenomenon has completely changed the game in both the investment management industry and the broader financial services sector. Attacks on fund managers, investment advisers and other fiduciaries ("Fund Managers") are increasing in frequency, sophistication and severity. And both the regulators and the investor community have been paying close attention. To responsibly manage Cybersecurity risk, Fund Managers need to, at minimum: (i) understand certain existing legal obligations and an evolving regulatory focus; (ii) comprehend fundamental IT and technology principles; (iii) monitor evolving threats, technologies and attack protocols; (iv) appreciate its data use and information work flows; and (v) simultaneously manage its employees' training needs, its vendor controls and its investors' expectations. Align Cybersecurity™ solves all of these challenges.

As it stands today, Cybersecurity law consists of a crazy quilt of federal, state and international laws and statutes, which are further complicated by additional industry-specific rules and best practices, together creating a body of jurisprudence that is disjointed and convoluted. Similarly, since early 2014, we've seen regulatory initiatives demonstrating that Cybersecurity is squarely in the crosshairs of investment management regulatory bodies, including the SEC. Examples include the SEC's recent "Cybersecurity Sweeps," its triaging Cybersecurity as a top regulatory priority for the last four (4) years running and its recent enforcement actions activities, which have induced at least one seven-figure settlement.

And yet the elements of constructing a model Cybersecurity Program remains unclear, leaving Fund Managers struggling to understand their legal, compliance and fiduciary obligations.

"Clearly, 'Cybersecurity Preparedness' is viewed by the regulators as both a core control and a minimum standard, yet one which they refuse to define," says John Araneo, managing director, Align Cybersecurity, and general counsel of Align. "The guidance provided to date has been largely principals-based, failing to provide a clear construct on precisely how to design an unimpeachable Cybersecurity Program. Unfortunately, in the absence of any bright line rules or black letter law espousing the required elements of a sound Cybersecurity Program, Fund Managers have been left scratching their heads on how to comply."

John Araneo, managing director, Align Cybersecurity

Vinod Paul, COO of Align

Cybercrime has evolved into a vexing cat-and-mouse game: criminals make a move, you counter it, they counter your counter, while damages accrue. Cybercriminals don't just target technology, they target human flaws through myriad vectors of attack, including phishing, business email compromise (BEC), malware and ransomware. WannaCry and other devastating ransomware outbreaks have taught the world that cybercriminals gain an upper hand due to a false sense of security, lack of training and obsolete systems. Fund Managers must remain informed of these emerging and evolving risks as they develop.

"In the new era of Cybersecurity where threats are omnipresent, Fund Managers require a comprehensive solution that enables firms to stay one step ahead of cybercriminals," says Vinod Paul, COO of Align. "Align launched Align Cybersecurity specifically to fill this void in the investment management space and recently assembled an elite team of Cybersecurity subject matter experts encompassing legal and compliance, IT and technology and security protocols. Our Cybersecurity Advisory Services offer an unparalleled suite of solutions, helping Fund Managers design customised Cybersecurity Programs that will satisfy regulators, please investors and empower employees." ■

9 ▶ making progress? And what do you need in terms of budget, six to 12 months from now? Demonstrate what you've done, and, if it's not enough, justify what budget you need to complete the task. It's all about doing what is most appropriate from a planning perspective."

Of course, the problem with ransomware, by way of example, is that it takes place in the background. The latest file-less malware strains will try to figure out what software is being used on a system and then attempt to disable updates, leaving computers vulnerable to future attacks.

Sprickerhoff notes that one ransomware group is locking databases and saying, 'We'll let you restore three workstations, which three are they going to be? And by the way, we've locked your database so it's going to cost you more to get that data back'.

"Depending on the database, the client might find themselves having to negotiate thousands of dollars. This is a very tailored approach to malware attacks," says Sprickerhoff.

If someone suffers a cyber breach, having good detection tools in place will help to identify an attack early on and give the manager time to respond. Then it boils down to: Have you got the right playbooks to know how to respond? Have you practiced them?

"Any organisation that is systemically important needs good cyber hygiene that covers entry level defence, targeted protection around your most valuable assets, detection systems that pick up anything that doesn't look normal for your network, and a clear response policy, which means knowing what steps to take to contain the threat.

"People like to spend budgets on fancy systems with flashing lights while completely missing some of the basics of cybersecurity," asserts Balding.

Sprickerhoff says that eSentire recommends that every quarter clients run tabletop exercises to test their incident response plans, "because things are constantly changing. Maybe not the entire IRP but certainly a sub-set of it. You want it to be a live document, not something gathering dust on the shelf."

As fast as the cyber threats evolve, there is one constant feature one can be sure of: the human.

"The older generation are perhaps a little blasé and less educated on the sophistication levels of cyber attacks. In addition, I think this has a direct impact on the policies that a firm will employ."

Dean Hill, Eze Castle Integration

No matter what the size of a breach, or the technology being used to guard against it, people will always be the weakest link.

The most common aspect of social engineering is the phishing campaign. Dean Hill is Executive Director, Eze Castle Integration. He says that, in relation to cyber hygiene, the biggest issue for firms to deal with is continuity. Often, they will embark on a process to improve their cyber security framework, including staff training, and will sessions once, twice, before it becomes a bore and they forget why they are doing the training in the first place.

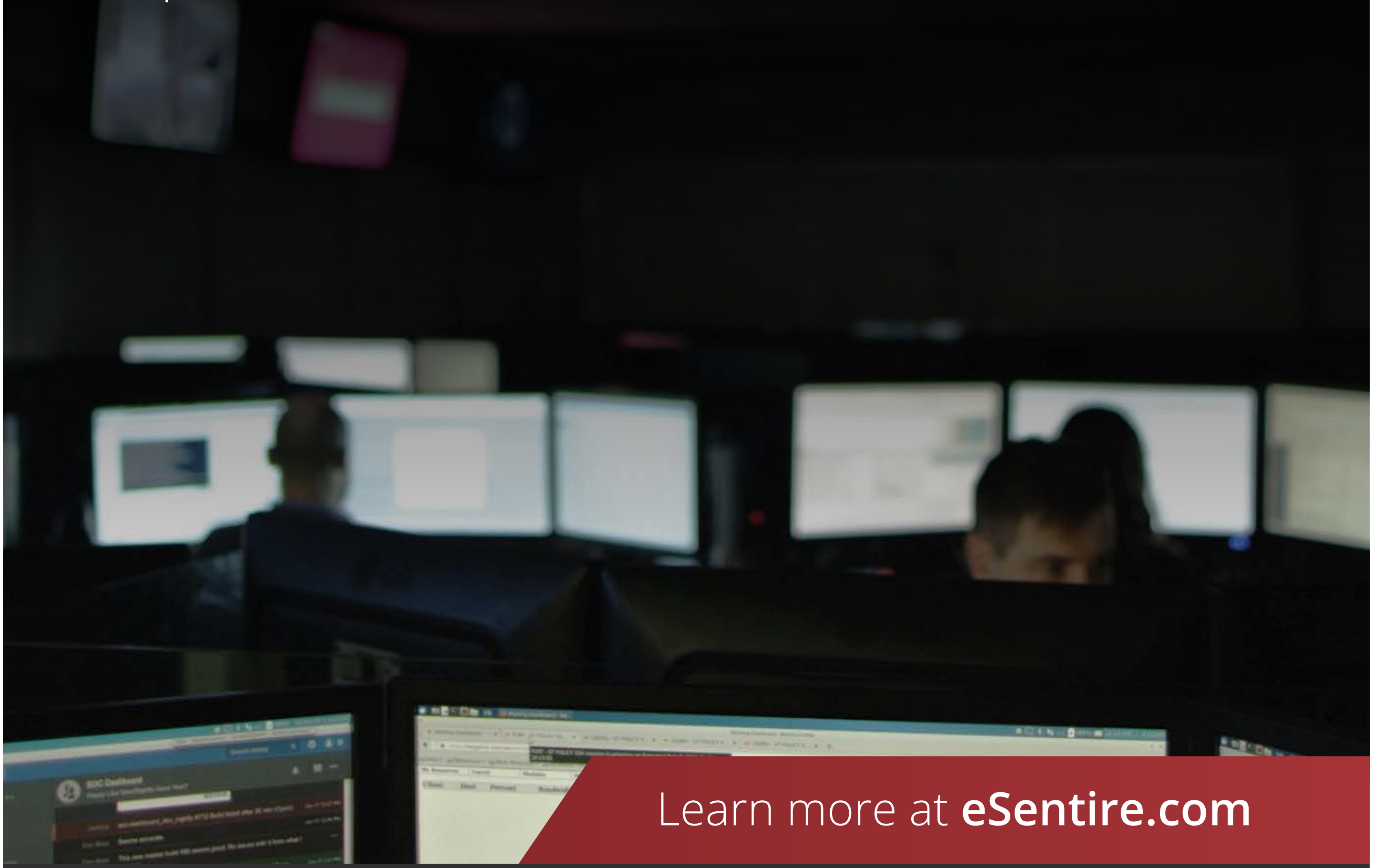
"Everything we tend to see in relation to phishing involves a lack of human training. Typically, it is the senior people in organisations that are targeted. These are well constructed attacks using social engineering, a lot of research goes into them, and the rewards are often substantial.

"The older generation are perhaps a little blasé and less educated on the sophistication levels of cyber attacks. In addition, I think this has a direct impact on the policies that a firm will employ. If you've got C-suite executives that are not fully up to speed and don't fully appreciate the risks, they are less likely to correctly enforce any policies or procedures, and in that instance, we, as a technology firm, are fighting a losing battle.

"Put a plan in place and stick to the process. Ultimately, you don't do something for nothing. You have to reinforce why it is important," states Hill.

Having a one-size-fits-all approach to cyber awareness training is akin to throwing money down the drain. According to Balding, firms should segment their employees into different groups based on risk profile.

▶ 17



Ransomware: Managers should expect the unexpected

Interview with Eldon Sprickerhoff

Ransomware, malicious code that encrypts files and demands a ransom to decrypt, has been around for years, but why is this most recent version so successful? The answer is bitcoin. Bitcoin provides a method by which hackers may remain anonymous yet still have a way to monetise attacks without creating a money trail. But whereas most public ransomware attacks to date have tended to be low-scale and relatively unsophisticated, the Internet of Things means that billions of devices are now connected, presenting a surfeit of attack surfaces for cyber criminals.

Not only that, but the ambition of ransomware attacks has grown, as evidenced by the WannaCry event last month, which caused chaos, infecting some 300,000 computers globally.

"The most recent SEC-OCIE Risk Alert highlighted the fact that ransomware was a particularly important issue upon which firms must focus; something that I have long advocated. But there's still so much to look at because there are new versions of malware constantly evolving, week-by-week," comments Eldon Sprickerhoff, founder and chief security strategist for the cybersecurity services company eSentire Inc.

For any fund manager, probably the most important question to ask when conducting a due diligence appraisal of their service providers, is 'What are you doing to defend yourself against ransomware?'

This might appear a simple question but consider what it takes for a ransomware attack to be successful. Approximately a dozen things have to go wrong in serial for a ransomware attack to be successful.

Eldon Sprickerhoff, founder and chief security strategist for eSentire Inc

There are technical aspects, such as email servers (both local and that of a upstream mail service provider) failing to detect the malware; there are training issues, where an employee received the malware email, clicked on it and initiated the attack inadvertently, the lack of an incident response playbook to follow, or even a backup methodology that doesn't fit the current needs of the firm.

"Given that ransomware is a highly likely attack vector, the more fulsome a response a firm can offer their clients the better. It will give managers a pretty good sense of how well placed the service provider is to defend almost all types of cybersecurity attacks. Defence methodologies used against ransomware improve a firm's defence against insider threat, other malware threats, data extrusion threats and so on. That one question, simple as it is, covers a whole array of technical and policy/procedure considerations," says Sprickerhoff.

To help with this, eSentire has developed a ransomware defence matrix*, detailing which mechanisms to put in place to guard against a ransomware attack.

With respect to WannaCry, it only impacted organisations who had failed to do a patch update that Microsoft had released a couple months prior to the attack.

Microsoft runs a patch release program called Patch Tuesday; something they've been doing every month since October 2003. This March, things were different. There was more urgency. Microsoft sensed that an attack was imminent and needed to get the patch out quickly, not wait until the second Tuesday of the month.

"Even though Microsoft said these were critical patches, there didn't seem to be the heightened concern that it truly demanded and some firms treated it like any other critical patch that could wait for whatever their regular patch cadence required. In some cases, this could postpone the installation until the next quarter. Suddenly you have a scenario where firms could be susceptible to weaponised zero days discovered by the NSA," says Sprickerhoff.

There is some concern that a similar ransomware attack could bring down global exchanges and hobble the financial industry. Sprickerhoff refers to the Sapphire worm from 13 years ago.

"It was a vulnerability discovered in Microsoft SQL; once infected, it rattled through data providers and financial institutions, flooding networks and shutting down banking machines. We are, however, so much further ahead and better protected than we were 13 years ago. I recommend that financial organisations of all sizes re-assess their incident response plans following WannaCry."

Email remains the most favoured attack vector for ransomware. It has, however, moved on from people emailing executables to a stage where malware has become essentially fileless.

Rather than directly download a malicious piece of code an attacker may use an different vector, such as the use of 'Powershell' to download and execute code. Similarly, malicious content embedded in a benign document, such as a macro may be more difficult to discover.

"A user may open an Office document which runs the embedded macro and inadvertently downloads the malware onto the terminal. A typical antivirus programme may not necessarily going to catch it; at a high level, this is how infection vectors have changed in the last few years and antivirus programs have not all caught up," concludes Sprickerhoff.

Financial institutions are probably better protected than any other industry but as WannaCry showed, they still have to expect the unexpected. ■

www.esentire.com/resources/workbooks/ransomware-defense-matrix

Risk assessing outsourced IT partners

Interview with Viktor Tadijanovic

The average hedge fund is often a lean operation with limited headcount, which leans more towards the front office. As such, areas such as IT and cybersecurity are typically outsourced. Many have chosen not to hire CISOs but have instead chosen to appoint outsourced partners/consultants to conduct risk assessments, including appraising the manager's third party vendor relationships.

"We are one of the largest counterparties to some of our clients: we provide their IT, we are custodians of their data and we provide systems that enable them to run their business," comments Viktor Tadijanovic, Founding Member and CTO of New York-based Abacus Group. "We are their outsourced IT platform and we provide a number of cybersecurity controls and technologies. Given the number of high profile attacks, clients increasingly want to improve their cybersecurity posture to put their house in order."

One of the main reasons for embracing the outsourced IT model is that the costs of building and maintaining internal technology resources is prohibitively expensive, given the amount of compliance and regulatory requirements that hedge funds face today. However, this means that proper checks and balances need to be in place when using a third party IT vendor.

Evaluating a client's IT partners, like Abacus, includes looking at the investment they are making in cybersecurity, as well as the transparency they provide.

"The nature of the service we provide is a black box. Everything works but the client doesn't know how it works. Consequently, lot of work is done providing a window of transparency into that black box to show clients our controls and make ourselves accountable. We continually make investment into those areas," confirms Tadijanovic.

Viktor Tadijanovic, Founding Member and CTO of Abacus Group

He adds that one of the challenges that IT service providers face is that there are, as yet, no industry standards and guidelines in place.

"We try to get ahead of this by providing a set of documentation that anticipates what our clients will want to know about us," explains Tadijanovic. "We go through an annual SSAE 16 audit, which produces a System and Organisation Controls (SOC) report outlining our controls and practices. We produce a standard document for each client that describes our technology and our controls. We have completed and routinely maintain the AITEC questionnaire, which we make available to mutual clients upon request. We also use some open standards such as SIG for information gathering. Standard Information Gathering is one of the emerging standards and provides some good guidelines on how to perform due diligence."

The SIG questionnaire, produced by industry body Shared Assessments, is essentially a holistic tool for risk management assessments of IT and cybersecurity. Tadijanovic confirms that Abacus have partnered with Shared Assessments and have purchased the rights to use their questionnaire.

"We fill out their questionnaires, covering all the different controls from human resources hiring practices to technology, back-up disaster recovery plans, etc. We also bring in third parties to evaluate our security posture three times a year. They do a penetration test and issue a report, which we also make available to clients," states Tadijanovic.

Tadijanovic concludes that the aim with all of these reports is to teach each client how to use them "to improve their security stance, so that if the regulator or an investor visits them, they know what to say". ■

12 ▶

"Anyone at the top table – the CEO, CFO, COO – will need different training to the rest of the organisation. Then you've got high visibility users – the ones that can be easily found on LinkedIn, who are more likely to get targeted by a cyber attack, and therefore need their own cyber awareness training."

Ultimately, every incident response plan should have clear instructions on how to report a phishing email. What does it look? When did it happen? What were the contents of the email? Then, there needs to be a proper notification process within the firm – who do you go to when you've identified one of these emails?

"A lot of firms that we work with don't have a process for this so that an employee knows who to forward the email to to check a link, or an attachment," confirms Hill.

There has to be a clear path of verification to determine what a potential attack looks like.

Each individual within a firm should know how to respond properly to a potential threat and escalate it accordingly, rather than clicking on something and putting the business at risk, especially from an outsourced perspective.

"If the manager outsources their IT and does not have internal staff who can deal with this, the employee needs to know what steps to take to share with their outsourced IT partner.

"Ultimately, as the first line of defence we would have done everything possible to identify and quarantine emails to check their contents before they reach the client. We have intrusion detection and prevention systems in place for this. We hope we will catch anything in the net that might contain a malicious attachment or link.

"If something malicious slips through the net, they just need to call us, email us; whatever is easiest. The last thing someone should do is forward the email internally to ask other people to check," advises Hill.

Balding provides a stark insight into the evolution of cyber attacks, using the banking industry by way of example.

Early on, organised crime chased after retail channels. They would focus on consumer accounts, and it was a high numbers game.

"In the space of a few years, malware has evolved from attacking retail accounts to corporate accounts to attacking the banks as a whole."

Craig Balding, Resilient Security

Then they started to climb up the value tree and target corporate banking channels, applying a lot of the same kind attacks but cashing out much larger sums of money. It became a lower volume, higher stakes game.

"They were using malware to get onto an end point workstation of a bank employee and installing software that would allow them to watch what that person did on the screen. The end result being that they could work out how to initiate a money transfer from one of the corporate employees. They took time to sit in the background and learn what the employee was doing. It works well because it was scalable; you only needed to learn the bank platform application once before replicating it multiple times with different banks.

"The third level of sophistication is the SWIFT attack. Now we are talking about the ability to move significant sums of money from one bank to another. In the space of a few years, malware has evolved from attacking retail accounts to corporate accounts to attacking the banks as a whole," says Balding.

The Bangladesh central bank heist last year saw USD81 million appropriated in what remains, to date, the largest cyber heist.

Going forward, Tadijanovic thinks that artificial intelligence will play an increasingly important role in terms of helping firms spot patterns in metadata: possibly a signature of a cryptovirus or a data exfiltration by a disgruntled employee.

"We are focused on this area right now to help us to harness data and make sense of it. It's beyond the capacity of the human brain to consume and make sense of huge volumes of data and come up with the right cybersecurity policy decisions," concludes Tadijanovic. ■