NEW CYBER RISKS
Remote working leads to increased vulnerabilities

ARTIFICIAL INTELLIGENCE
Proactively detecting threats with greater use of automation

STRENGTHENING SECURITY
Policy review, training and communication vital to success

Featuring Richey May & Co | RFA
Accounting
Assurance
Tax
Management Consulting
Technology Solutions

RICH'EY
MAY & CO

Full-Service Solutions & Resources for Alternative Investment Professionals

Our team combines the dedicated expertise found in a national accounting firm with the hands-on approach to client service you’d expect from a boutique provider — a unique model that allows us to bring expert solutions and strategies to your specific business needs.

Learn more about us and see the latest resources from our team, including a complete Guide to Fair Valuation under ASC 820, on our website.
INSIDE THIS ISSUE…

04 WORKPLACE FLUIDITY LEADS TO GROWING CYBER VULNERABILITIES
By A. Paris

08 PROACTIVELY DETECTING THREATS THROUGH AI
Interview with John Thomas Gaietto, Richey May & Co

10 STRENGTHENING SECURITY THROUGH POLICY REVIEW, TRAINING AND COMMUNICATION
Interview with George Ralph, RFA

12 DIRECTORY
Hedge funds and alternative asset managers are responsible for over USD3 trillion in assets under management—many bright shiny diamonds for cyber criminals to pursue. Increased levels of remote access propelled by the Covid-19 pandemic are making these organisations even riper targets. So, in this environment, the cost of inaction or complacency around cybersecurity continues to mount.

According to IBM Security, the average cost of a breach within financial services is of USD5.85 million—this is well above the overall average of USD3.86 million per breach across all industries reviewed. Although the crisis has put many managers under pressure in terms of budgets, continuous review of cybersecurity systems should not be left by the wayside.

A heartening argument in these belt-tightening times is that the amount of money firms dedicate to cybersecurity is not necessarily a measure of a system’s success. In fact, a study by Deloitte concludes that the way a programme is organised and governed can be equally, if not more, impactful than how much a firm spends on cybersecurity.

Infrastructure and investment
The study discusses firms’ cybersecurity programmes according to their maturity level. Within adaptive firms, leadership drives the cybersecurity agenda. The report finds: “Almost all board and management committee members at responding companies were keenly interested in their company’s overall cybersecurity strategy. However, those from adaptive companies suggest their boards are more likely to delve into the details of the cybersecurity budget, specific operational roles and responsibilities, as well as the programme’s general progress than are boards of less advanced peer companies.”

The consultancy also partnered with the Financial Services Information Sharing and Analysis Center (FS-ISAC) to survey its members. This association is dedicated to reducing cyber-risk in the global financial system. Survey respondents reported an increase in cybersecurity spending, with identity and access management, cyber monitoring and operations, and end-point and network security receiving bigger shares of the pie.

Workplace fluidity leads to growing cyber vulnerabilities
By A. Paris
Pandemic impact
The Covid-19 pandemic accelerated digitisation and remote working arrangements across the financial services industry. Firms with strong technology architecture were arguably in a good place to make this transition. However, the FS-ISAC report notes: “This sudden shift has compounded problems for many chief information security officers (CISOs) and cybersecurity teams charged with securing the digital fortress at their firms. Hackers and cyber scammers are trying to take advantage of expanding technology footprints and new attack surfaces, with most employees working remotely.”

JP Morgan Asset Management warns clients: “Periods of crisis bring out the best in humanity, but the worst in online scammers. Now is the time for extra vigilance when accessing your investments online, responding to emails and managing personal data.” The firm says that in addition to employing the latest fraud prevention strategies and technologies internally, it is committed to providing useful information that empowers clients to take control of their own cybersecurity.

A report by PwC remarks: “As many organisations within the asset and wealth management sector have adapted to virtual working environments, there is a need to be more vigilant than ever when it comes to cybersecurity awareness. With so much capital at stake, in a sector that is guided fundamentally by risk appetite, it is vital that organisations within the sector maintain and uphold a robust, secure environment, as well as have the capability to detect and respond to attacks such that the business impact, if any, is minimised.”

The FS-ISAC report warns: “Financial institutions should be particularly judicious before making a reduction in cybersecurity budgets. Given the increased push toward digitisation and the challenges raised by new, often remote work environments, as well as an increase in insider threats, cyber risks confronting most organisations are intensifying.”

Vulnerabilities
The increased levels of remote working have undoubtedly also led to rising vulnerabilities on behalf of manager organisations.

“When someone logs into their workplace from home, they’re using the same device – most likely their mobile – that controls access to their personal networks, including their digital assistant, smart television, smart refrigerator and even their connected car,” says Macquarie Capital managing director, Tej Shah. “Each of these devices is, in turn, connected to thousands, potentially millions, of additional devices through the apps and the software they use.

“When you couple that with machine learning, which can leverage phishing as an attack method more easily, especially at the individual level, you can see how the perimeter quickly becomes nebulous, making it easier for a hacker to get into a company’s system through a single point of weakness.”

PwC analysts note a rise in human operated ransomware and data exfiltration attacks. Although there is no data to directly attribute this increase to the Covid-19 pandemic, the correlation cannot be ignored. “The statistics support the hypothesis that the increase in publicly known threat actor activity is a direct result of the current economic downturn,” they say in a report.

In such attacks the malicious actor would have completed an in-depth reconnaissance exercise ahead of deploying ransomware on the target. The information collected is then used as leverage against the target firm, with threats to release any confidential files onto leak sites.

As of 20th May 2020, PwC observed over 150 organisations in the asset and wealth management sector around the world having had their data leaked in this manner by multiple threat actors. “With the sector being a lucrative target before individual countries began instigating their national lockdown policies, the abrupt adoption of remote working technologies alongside threat actors growing more emboldened, presents new cybersecurity challenges at this time,” the consultancy says.

“We see cybersecurity as an increasingly important risk for all investors to monitor, with implications that cut across sectors, from financials to utilities.”

Scott Thiel, BlackRock
Outsourcing expertise

Much has been said about the rising salaries cybersecurity and specialist IT executives command. This is partly driven by the fact that there aren’t many of these individuals around. The (ISC)² an international, nonprofit association for information security leaders estimates the current cybersecurity workforce at 2.8 million professionals. However, the association also identifies a significant shortage as it says the industry needs an additional 4 million trained professionals to close the skills gap.

According to a report by Allied Market Research, the managed security services market overall is expected to grow to USD40.97 billion by 2022. George Ralph, managing director at RFA comments: “We have definitely seen an uptick in demand for fully outsourced and managed cybersecurity services delivered via our Security Operations Centres (SOCs). I believe a combination of increasing regulatory and investor pressures, increasing velocity and ingenuity of attacks, a lack of available skills and the natural move to outsourced services has led to this.”

John-Thomas Gaietto, executive director of Cybersecurity Services at Richey May & Co highlights the importance of quality when considering external partners and enterprise tools: “If you’re looking at second or third tier provider, odds are they won’t have the sophistication or tools available to enable you to protect your environment in a cost effective and efficient manner.”

The investment angle

Aside from managing the operational threat of cybersecurity concerns, managers are also looking at the sector as an investment opportunity. For example, Robeco began to involve a cyber expert in its investment process a few years ago. The “white hat hacker” was brought in to investigate the degree to which companies Robeco invests in might appeal to hackers and help identify which business units are at risk.

BlackRock, also considers cybersecurity in its investment process. In an insight piece Scott Thiel, BlackRock’s chief fixed income strategist says: “We see cybersecurity as an increasingly important risk for all investors to monitor, with implications that cut across sectors, from financials to utilities.”

A firm that has taken this a step further is ForgePoint Capital; it focuses on investing solely in emerging cybersecurity companies. In February this year the firm announced the close of its second fund with USD450 million in capital commitments. This is the industry’s largest fund focused exclusively on cybersecurity and will invest in early-stage and select growth companies.
hedgeweekLIVE
EUROPE
DIGITAL SUMMIT
HOSTED BY hedgeweek

KEY STEPS TO SUCCESS

11-12 NOVEMBER 2020

for more info contact events@globalfundmedia.com
Artificial intelligence is enabling organisations to be more proactive in their approach to cyber threats. Work environments with greater levels of remote access could be deemed more vulnerable, but the element of automation in identifying and remediating potentially malicious behaviour provides a superior measure of security.

A key development in the realm of cybersecurity has been the creation of end-point detection and response or EDR.

John-Thomas Gaietto, executive director of Cybersecurity Services at Richey May & Co discusses this progress and the benefits it brings firms: “The general basis of the tool is that, unlike traditional malware software that requires definition files to function and detect threats, this solution utilises machine learning and behavioural analysis to detect malicious behaviour.

“This technology enables organisations to detect threats earlier. Further, these tools have a lot of security automation built in. So not only can you detect the threats sooner, but you can also respond and remediate near automatically. That really moves the needle for a lot of organisations.”

In debating the enhancements artificial intelligence has facilitated within cybersecurity, Gaietto refers to repeating patterns: “There are things that humans wouldn’t pick up on because of the volume of information they would need to analyse. AI allows organisations to identify anomalies and behaviours that would have been much more difficult to isolate without that automation.

AI and other automation can give a lending hand to organisations which do not have the budget for an around the clock security operation centre. “Instead of alerting a cybersecurity person and having to wait for them to check their phone, the tool can automatically take an action to stop the spread of any malicious behaviour. The system dictates the action taken when it detects certain type of behaviour,” Gaietto explains.

The industry talks about preventing zero-day attacks and in a world where large swathes of the workforce are operating from remote locations, this takes on greater significance. According to Gaietto, in addition to EDR tools, one of the crucial elements in protecting an organisation is frontline defence, especially when confronted with phishing attacks.

“The first protocol should always be education. Communicate with your employees, as they are your first line of defence. When writing your policies, don’t threaten to penalise people for stepping forward or reporting. You want to encourage them to do that. The companies that invested in training have seen the volume of frontline reporting increase dramatically. So that investment does pay off,” Gaietto advises.

Secure configuration
One of the things financial firms need to wary of is trying to take a traditional cybersecurity approach into the cloud. “You really have to understand the methodology on how to configure the cloud in a secure manner,” Gaietto says.

This is important because many of the major cloud providers work on what is called a shared responsibility model. This means they protect the physical security side of things. But the organisations themselves are then responsible for configuring the environment to protect their workloads and data.

Getting this right is crucial as it can make or break the solution
RICHEY MAY & CO

John-Thomas Gaietto
Executive Director of Cybersecurity Services, Richey May & Co

John-Thomas Gaietto, CISSP, has more than 22 years of experience providing enterprise information security and risk management services to a variety of organisations. His expertise includes the development of security strategies based on organisational risk, oversight of security operations, incident response, third-party risk management, disaster recovery, and building high-performing Information Security teams. His experience includes numerous compliance verticals, such as PCI-DSS, Sarbanes-Oxley, HIPAA, GLBA, FISMA, TPN, ISO, SOC, New York State Department of Financial Services Data Security and GDPR.

and its deployment. According to Gaietto, in most of the headline stories outlining cloud breaches, the root cause is usually user error in configuring the solution they’ve adopted from the provider. “It is very rare that it’s a software vulnerability issue. Typically, it’s due to user error,” he says.

Partnerships and impact analyses
Gaietto goes on to outline the benefits of appointing a third-party partner to manage cybersecurity: “It’s simple economics; it’s about the demand and the cost. We’ve seen salaries of cybersecurity staff really skyrocket over the last two or three years, so often it doesn’t make sense for an organisation to have an in-house cybersecurity team which is not a hundred percent utilised a hundred percent of the time. A third-party provider, on the other hand, can provide the service to multiple clients at the cost of half or three quarters of one expert’s salary.”

Also, firms need to understand which areas of their business they should focus on when putting together their cybersecurity strategy. In order to determine which processes or areas of business are critical from a cybersecurity perspective, a firm should undertake a business impact analysis. This means talking to different stakeholders within the business to understand the processes and systems that are essential to their particular area of work.

“An exercise like this identifies business processes and how critical they are to the operation of the organisation. For example, in HR and payroll – if certain processes or systems are compromised, then employees run the risk of not getting paid. Therefore, in this case these are vital for the smooth running of an organisation. Following that, the organisation can map out its technology needs and understand which are the critical or vulnerable parts of its network. These will be the areas they should prioritise when putting together a resiliency programme or disaster recovery programme,” Gaietto recommends.

Strategic planning
This element of strategic planning is one Gaietto believes the industry should focus on: “The compliance side of business resilience is going to be vital going forward. Not many organisations have a defined plan going into the pandemic, and while they made it work, it was all a bit knee-jerk and done on impulse. We are really pushing hard on companies to have clear strategies in place to better protect customer information and things of that nature.”

Mapping out a clear path ahead is even more important in the current environment, given the uncertainty as a result of the Covid-19 pandemic. “Most organisations are going to come under strain due to a lack of economic activity. Therefore, as budgets get leaner and there is less room for error, making efficient use of that budget is going to become even more important,” Gaietto notes.

He concludes by saying many firms still have a lot to accomplish when it comes to the adoption of automation, AI and machine learning: “This is going to play a huge role. It’s a trend that will continue, because it can be implemented without having a dramatic impact on a firm’s operating cost, which has considerable appeal at this particular point in time.”
Firms can have a belts and braces approach to the security of the systems and tools they deploy, but staff training and communication can make or break their chances of success.

“We recommend overhauling policies and procedures, and implementing these via training which happens at induction and regular points thereafter,” advises George Ralph, managing director at RFA.

Cybersecurity has become a board level concern and many clients now prioritise it in their risk register. With SMCR reigniting its importance and responsibility, cybersecurity now also features heavily as a standard element in every ODD exercise. Essentially, if the investors are asking about it, fund managers have to prioritise it.

How far along the spectrum of cybersecurity a firm chooses to go depends on their risk appetite. Ralph points out: “Some firms have a very low risk appetite and require the full portfolio of device and network security tools, user training and penetration testing. They would need a full rewrite of policies and procedures, locked down devices, a ban on external USB drives, no downloads and locked down printing.

“We would always undertake a risk management analysis exercise to understand what the client is trying to achieve and how low their appetite for risk is, versus their budget and expectations. The key is also ensuring you adapt the solutions to the working patterns of the team. For example, if you have a fully remote workforce you need to ensure that the tools are protecting them in a zero trust approach without preventing work efficiency. You also need to enable proactive issue detection on the end-points as they may not have immediate access to technical support.”

The industry progression from intrusion detection to prevention is an important step to highlight. Detection can be considered quite a passive practice, with firms waiting for the intruder, detecting that intrusion when it happens and only then taking action. "This is the old way of doing things," says Ralph, “Our systems are proactive, continually scanning and assessing the network but more importantly, the end-points, to identify and highlight activity that may be deemed as preceding an incident, or that is anomalous - even in the smallest way, and could lead to an incident.

“The fact that we monitor the end-points is very important given the current remote working situation. It supports the almost certain move to a hybrid working environment, whereby users will be working in a combination of ways, some permanently remote, some using the office occasionally and others back in the office full time.”

The end-point monitoring and detection solution by RFA uses AI enabled tools to identify patterns or behaviours that may be deemed anomalous and take action, regardless of whether the device sits inside or outside of the corporate network.

“AI enabled ops tools are very important across the IT estate, especially where automation is concerned. If key workflows and business processes can be automated intelligently, using AI tools, firms can benefit from cost and time savings. They can also see higher accuracy rates and more timely processes,” Ralph comments, “This is particularly relevant when looking to meet regulatory obligations since accuracy and efficacy are particularly crucial in this context. Removing that human element from some processes means reducing risk or both key man dependency and human error.”

George Ralph CITP, has successfully founded three technology firms along with C-level advisory services include M&A to numerous firms. George is a true leader and has been managing teams internationally, and leading technology transformation projects for over 20 years. A certified GDPR, Cyber assessor, Auditor, Architect and widely experienced cybersecurity and RegTech professional, George has extensive technical experience in network and server architecture, large scale migrations utilising leading technology brands, and IaaS offerings.
World-class technology services for hedge funds

› Managed Cybersecurity and Compliance
› Cloud Services
› Workspace and Collaboration Solutions
› 24/7/365 IT Services and Support
› Managed Data Services
› ODD Support
› Business Continuity Practice

Whether you're operating locally, nationally, or internationally, RFA has offices around the world and is your global technology partner

www.rfa.com
gralph@rfa.com

The Trusted Technology Partner

London | Luxembourg | New York City | Boston | Connecticut | Westchester | San Francisco | Singapore
RICHLEY MAY & CO
Founded in 1985, Richey May & Co. provides accounting and assurance, tax, management consulting and technology solutions to clients throughout the United States. As a public accounting firm with hundreds of Alternative Investment clients in over 40 states, Richey May has a depth of specialized knowledge few firms can claim. Our team combines the dedicated expertise found in a national accounting firm with the hands-on approach to client service you’d expect from a boutique provider – a unique model that allows us to bring expert solutions and strategies to your specific business needs.

Our knowledgeable staff of over 200 employees, including 17 partners and over 150 professional staff, is dedicated to introducing new and innovative ways to exceed our clients’ expectations.

Contact: Eliza Barry | eliza@richeymay.com | +1 303 721 6131

www.richeymay.com

RFA
RFA is the technology partner to alternative investment firms who require end-to-end cloud, cybersecurity, infrastructure and application solutions. RFA is a global, next-generation MSP with a distinguished 30-year pedigree

Unlike other industry offerings, RFA does not put firms “in a box”; its culture of innovation and thought leadership empowers businesses to compete how they want to – securely.

Contact: George Ralph | sales@rfa.com | +44 (0)20 7093 5000

www.rfa.com