STAFF TRAINING
A vital element to any cyber-security framework

CLOUD TECHNOLOGY
Private and public both viable options for funds

UP-TO-DATE SOFTWARE
Regular updates essential for an effective firewall

FEATURING Ace IT // Capital Support // Eze Castle Integration // eSentire // Matsco Solutions // McGladrey // netConsult // Options IT // Dell SecureWorks
What’s keeping you up at night?

CYBERSECURITY

You are not alone. The SEC, SIFMA, FINRA, DHS and multiple other organizations are worried about the threat of cyber attacks and vulnerabilities like ShellShock.

eSentire is the leading provider of continuous active threat protection to the financial services industry. We’ve helped numerous clients exceed the expectations of regulatory associations while protecting their assets and investor interests 24x7.

We can help. Contact us today:
1.866.579.2200 | sales@esentire.com
http://info.esentire.com/sec-exam-readiness/
The threat of a cyber breach has become increasingly acute in the past year. Criminals are constantly creating more innovative hacking tools with which to attack a fund’s valuable and sensitive data.

A string of high-profile cyber-attacks in 2014 highlighted the stark reality that, for the financial industry especially, dedicated cyber defence systems are no longer a luxury; they are a necessity.

The SEC in the US is asking managers to show they operate cyber defence software and have implemented detailed action plans in the event of a breach, as part of its guidelines on the topic.

In this HFMWeek Cyber Risk and Security Report 2015 we hear from leading cyber service providers who discuss the key points surrounding creating an effective system. HFMWeek compares the pros and cons of creating a private in-house cloud platform against an outsourced third-party provider.

HFMWeek also discusses various best practices that industry specialists are recommending to hedge funds of all sizes, and the importance of mastering the basics of password protection and staff training exercises to avoid the many phishing attempts that will come.

Many cyber industry specialists now agree that attempted cyber breaches on funds of all sizes are now inevitable. The question of whether they’re successful is up to you.

Drew Nicol
REPORT EDITOR
SECURITY
FULL SPECTRUM SECURITY
Gustav Marx, service development manager at Matsco Solutions Group, discusses the top security solutions available to hedge funds

TECHNOLOGY
ARE YOU REALLY SAFE?
Mark Sangster, vice-president, marketing, with eSentire, speaks to HFMWeek about the lessons that can be learned from 2014’s cyber events

TECHNOLOGY
PUBLIC, PRIVATE, OR A BIT OF BOTH?
Phil Ashley of netConsult discusses the public versus private cloud platforms and the factors that should guide a fund manager’s choice

CONSULTING
BE PREPARED
McGladrey's Alan Alzfan and Daimon Geopfert speak to HFMWeek about the reality of the threat facing hedge funds through cyber attack

TECHNOLOGY
GETTING STRONGER TOGETHER
Bob Guilbert of Eze Castle Integration explains why so many funds are opting for cloud solutions and how the industry can work together to tackle cyber crime

TECHNOLOGY
FEEL SAFE WITH MANAGED SECURITY
HFMWeek catches up with Marcus Lewis of Capital Support to discuss the company’s new cyber-security suite

TECHNOLOGY
STANDING OUT FROM THE CROWD
John Bryant, head of technology at Options IT, talks to HFMWeek about why the company’s offering is the clear choice for funds even in a busy financial marketplace

TECHNOLOGY
CHANGE STARTS FROM WITHIN
Warren Finkel, of ACE IT, explains why cyber-security must include a top-down approach to security awareness

TECHNOLOGY
THE ATTACK HAS EVOLVED, HAVE YOU?
Dan Bonnet, sales director, Dell SecureWorks, talks to HFMWeek about the must-have features of a cyber-security service provider
Security services and information technology systems are designed, tested and developed to help with the prevention of data loss, limit potential system compromise and to help prevent mid- to high-level security events from occurring within a company’s information technology environment.

The latest generation of security systems that are developed offer enhanced security services that are fully integrated within a growing family of shared technologies and knowledge bases that encompass and deliver the most up-to-date elements in regards to environment and system management.

Vendors and developers provide regular updates, security patch releases and software versioning as an integral functionality of these systems, strengthening the relationship between the central security knowledge base and control centres and the widely dispersed security units. All the different segments that make up the multitude of security systems are able to provide up-to-date industry specific security solutions to individuals and companies alike.

The continued development of these security patches, security software solutions and integrated hardware systems allow security staff the ability to implement, monitor and maintain security solutions suited to their individual environments to the highest available standards. This enables companies to identify and prevent malicious attempts to access sensitive data and private systems, and delivers the benefit of industry compliant solutions in an increasingly cyber security conscious work environment.

“Companies can, regardless of size and environment complexity, implement enterprise level security systems”

Gustav Marx, service development manager at Matsco Solutions Group has worked in IT services for more than eight years and is responsible for service improvement, infrastructure design, planning and product research. Focusing on cyber-security and cloud, Marx has developed a keen understanding of technologies available and methods of implementation.
security systems to manage and protect the data that requires dedicated protection in all transitory and fixed states from all possible threats; data integrity, data loss, corruption as well as internal and external access. To fully protect and maintain security within environments, these security systems are increasingly available in the marketplace, fully adaptable to different scenarios and customisable to suit any company’s budget, size and/or security requirement.

A mixture of these different technologies that are available today, allow companies to be proactive in their fight against cybercrime and enables security and compliance staff to put in place preventative measures that ensure enhanced security for the users and sensitive data that resides in their respective environments. These systems are currently available as several variations of hardware or software based solutions; pure cloud-based infrastructures, hybrid systems or fully dedicated onsite environments. Regardless of the method of deployment all these systems are able to offer the highest levels of security solutions that are currently available in the industry today.

There are many risks that threaten data security today and the increasing emergence and identification of pre-existing software loopholes, previously unnoticed exploitable routes into sensitive areas and non-secure environment access points, have placed a large burden on compliance and security staff in many companies. These loopholes, access points and exploitable vulnerabilities that allow access to secure environments are vigilantly researched, tested and corrected by the mainstream security firms and software companies to remove these points of vulnerability from all environments.

The top security solutions range in price from the low hundreds to thousands per user per annum. Due to the increased requirement for cyber security reviews and cyber security solutions within the industry, it has become a minefield for many budget conscious companies to cross on how best to determine which product is best suited to their environment and what the best price for the right solution is.

DUE TO THE INCREASED REQUIREMENT FOR CYBER SECURITY REVIEWS AND CYBER SECURITY SOLUTIONS WITHIN THE INDUSTRY, IT HAS BECOME A MINEFIELD FOR MANY BUDGET CONSCIOUS COMPANIES

TOP FOUR SECURITY SOLUTIONS:

1. MALWARE, SPYWARE, ADWARE AND VIRUSES
   - Security solutions designed to identify, protect and eradicate threats that pose security risks to systems and data
   - Auto-update of heuristic and protection software system files
   - Continuous scanning of the environment for threats
   - Central management consoles and policy controls
   - System configuration and malicious code identification and prevention
   The top systems: Symantec endpoint protection
   - Trend micro anti-virus and endpoint protection
   - Message labs email protection services
   - Mimecast email protection and scanning

2. UNAUTHORISED NETWORK ACCESS
   - Network and IP address monitoring, security and scanning services to prevent unauthorised access. Intrusion detection and prevention services that monitor the network for access attempts, brute force attacks, DDos and network penetration attempts.
   The top systems: eSentire Network protection and monitoring services
   - Dell SecureWorks
   - Cisco Global IPS/IDS services on Firewall units

3. CONFIDENTIAL DATA LOSS, EMAIL AND MOBILE DEVICE MANAGEMENT
   - DLP and sensitive data protection systems prevent unauthorised movement of sensitive data out the environment by implementing security policies, access policies and filter lists to control and prevent unauthorised data transmissions. Mobile device management allows administrators to control data, application and system access from mobile devices, personal or company owned, across any internet connection.
   The top systems: Symantec Security Management suites
   - Airwatch mobile device management

4. UNAUTHORISED SYSTEM ACCESS
   - Dual factor authentication services, domain controller and system access controls prevent unauthorised use and access to company owned services, applications and data.
   The Top systems: Cisco ISE Systems
   - RSA Token based authentication
   - WSAD dual factor Authentication systems
   - Domain based control servers and access lists

5. SYSTEM MONITORING AND UPDATES
   - Uncontrolled software updates and security patching
   - System monitoring and incident management
   - Logging and identification

THE TOP 5 IMMEDIATE SECURITY THREATS:

1. MALWARE, SPYWARE, ADWARE AND VIRUSES
   - Introduced to environments through mail, unauthorised data transfers, websites and programs
   - Encapsulated as packaged software installed to devices or scripts and system files that run on system start-up
   - Registry configurable files and keys
   - File lockout and encryption to prevent access
   - Key logging, data capturing and data worms

2. UNAUTHORISED NETWORK ACCESS
   - Access is gained through unsecured network device ports and unprotected access routes
   - Access over SSL security flaws
   - Software and application backdoors and security flaws
   - Unauthorised access to physical devices

3. CONFIDENTIAL DATA LOSS AND MOBILE DEVICE MANAGEMENT
   - Unprotected mail and file transfer, low level encryption
   - Data extraction through mobile devices and memory sticks
   - CD/DVD burning
   - Unprotected Web access and social accessibility

4. UNAUTHORISED SYSTEM ACCESS
   - Password and User name compromise
   - System hacks
   - Wireless hotspot access and network connections
   - Unprotected terminal access

5. SYSTEM MONITORING AND UPDATES
   - Uncontrolled software updates and security patching
   - System monitoring and incident management
   - Logging and identification
Today's rapidly evolving threat landscape and compliance requirements demand smarter and more responsive security services.

Protect your network in real time with **Managed Security Services**. A simple and cost-effective way to limit potential threats and meet compliance mandates.

- Focused on Security Essentials
- Security Intelligence from IBM X-Force Threat Analysis Team
- Partnered with ACE IT Solutions
- Powered by IBM

Contact ACE IT Solutions for a free security assessment | 646-558-5575 | www.cybersecuritynyc.com
Mark Sangster has garnered experience at industry giants like Intel Corporation, Research in Motion and Cisco Systems. He has an excellent understanding of the customer and key verticals and has the unique ability to put himself in their shoes to see the service through their eyes.

Though his 20-year sales and marketing career, Mark Sangster has
last year’s breach stories taught us many things about the complexities of previously underestimated network vulnerabilities. The rise in sophisticated targeted attacks is challenging cyber-security methodologies. Industry experts have long suggested that perimeter security is essential cyber-security defence. We don’t dispute that the layers of technology that we use today all play an essential role in good cyber-security hygiene. But what today’s complex targeted attacks prove is that cyber threats extend beyond the perimeter. These attacks demonstrate how the perimeter can be permeated.

2014 IN REVIEW
We’ve seen an undeniable shift from advanced persistent attacks to advanced targeted attacks. While this new breed that we see today has a longer life cycle, they are incredibly effective. Less than 40% of the attacks we see are malware-based. Sophisticated cyber-attacks like phishing and watering hole attacks are dominating the threat landscape. These kinds of attacks expose the Achilles heel of perimeter defences – technology alone can’t prevent your employees from clicking malicious email links. Targeted attacks are driven by attack ingenuity.

2014 highlighted some of the most high profile, highly publicised and sophisticated cyber-attacks the world has ever seen. These targeted hacks shed light on what we have known all along – that without equally intuitive defence mechanisms the world’s data is highly vulnerable. 2014 was not just the year the internet broke, solidifying the fundamental shift in the cyber-security landscape, but it also marked a point in time when businesses big and small started to wake up to this new reality. Sony, Target, Home Depot and JP Morgan were just some of the more high-profile victims of these attacks. For most it was too late for repairs – the damage was done. The loss of highly valuable data, financial or otherwise, can mean the end of a business or worse.

The sources of new cyber-attacks are varied and growing, with perpetrators ranging from nation states to insiders. They include hacktivists/activists, terrorists, organised criminals and smash-and-grab thieves. Basically, anyone who wants to profit from stolen funds or information. Their targets include intellectual property, sensitive industry or merger and acquisition information, or bank account credentials. They may simply be looking to inflict website brand damage. And their targets will inevitably include your enterprise. If you haven’t already been infiltrated, it’s just a matter of time.

The attacks can take the form of an email with infected links (phishing scams) or other infected media. They might infiltrate an executive’s computer while it’s being used at home, or pose as a trusted source in an email message or phone call. Stolen mobile devices represent another opportunity for attack. Clearly these attacks are often creative and highly effective. As cyber criminality becomes more intelligent, so must the means to prevent them. More often than not, victims of these crimes are unaware they have been hacked until it’s too late.

THE EVOLUTION OF A CYBER-ATTACK

Active threat protection, which means eyes on glass reacting and responding to real threats and mitigating them in real-time, is the new standard enterprises need to adopt. Recognising the drastic shift in attack vectors, experts now propose a far more adaptive framework.

Active threat protection, which means eyes on glass reacting and responding to real threats and mitigating them in real-time, is the new standard enterprises need to adopt and deter them. Cyber criminals will always look for vulnerabilities, without them they will move on to the next target or spin their wheels making fruitless attempts. To adequately protect high value assets, enterprises must continue to evolve their security defences.
Isolation techniques – a trusted entity may need to be isolated to keep it secure from an untrusted system. Conversely, in the case of a trusted system, you need the ability to isolate an untrusted entity from the rest of its contents. That way you can run and observe the unknown code or content and safely handle any malicious attacks.

Whitelisting is another important security foundation, which can ensure that only trusted entities are allowed to operate on the system. A perfect example of this is the Apple App Store. With over 500,000 apps available, there is virtually no malware because all of the apps are whitelisted by Apple before they can be downloaded to any system.

Regular testing is an important tactic to ensure the integrity of your security is intact. An example of this is using ‘honeydocs’ – fake phishing emails that help to gauge the solutions ability to react and respond to cyber-attacks.

**RECOMMENDATIONS**

Previous industry guidance suggested a far more siloed approach to cyber-security. However, today’s threat environment, detection and response capabilities are more important than blocking and prevention. Continuous monitoring and analytics must be at the centre of the security platform with the capability to respond within seconds, before an incident occurs. An adaptive security architecture (ASA) is critical.

Because of the often unpredictable and targeted nature of these newer cyber-attacks, human intervention is required to detect and intercept sophisticated anomalies that technology alone cannot detect.

One of the key aspects of a successful security strategy is the ability to contain and isolate information. Keep the bad from the good, and the good from the bad.

Your enterprise could set up your own security operations centre (SOC). But do you want to?

Setting up an SOC is problematic, especially for companies who have a high asset value to employee ratio. There may not be an extensive IT department in place. Recruiting suitable expertise is difficult and a highly competitive market can make retaining it problematic. An effective SOC is costly to build, maintain and manage. Technology is constantly evolving with frequent hardware and software updates, necessary to defend against the ever-changing threat landscape. And if any one of these areas becomes a weak link, your CSO could become the chief scapegoat officer. Don’t let it be you.

If you haven’t thoroughly evaluated your security strategy in the past 18-24 months and continually tested its effectiveness, you are not only at risk, you are exposed and highly vulnerable – you may be infected now. An effective security strategy requires sound protocols, continuous testing and monitoring and talented security experts with the knowledge to identify real threats.

Continuous active threat protection is the only proven strategy to combat the complex, targeted threats ever-present in today’s cyber environment. Accessing security as a service and utilising the highest level of threat protection and white glove customer service is the most effective way to protect your business in 2015.

---

**CONTINUOUS MONITORING AND ANALYTICS MUST BE AT THE CENTRE OF THE SECURITY PLATFORM WITH THE CAPABILITY TO RESPOND WITHIN SECONDS**
No one understands the security concerns of the hedge fund industry better than Options. Our offering combines best practice cybersecurity building blocks with continued operational agility and rigour.

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

PHIL ASHLEY OF NETCONSULT DISCUSSES THE PUBLIC VERSUS PRIVATE CLOUD PLATFORMS AND THE FACTORS THAT SHOULD GUIDE A FUND MANAGER’S CHOICE

HFMWeek (HFM): What is the difference between private and public cloud services?
Phil Ashley (PA): There is an ever increasing range of service providers which offer private and public cloud-based IT services and solutions. With the emergence of public cloud services, such as Google Apps, Amazon Web Services and Microsoft Office 365, product developments and marketing material for cloud services can be a challenge to digest and the critical differences between public and private clouds can become blurred and lost in translation.

The foremost defining factor of a private cloud over a public cloud is in the nature of storage and access to corporate data and IT services. A private cloud solution will deliver an independent, isolated and discreet system with individual policies and access control mechanisms. They are clear, standalone, single-tenanted environments with defined ownership which leverage the service provider’s infrastructure.

Public clouds on the other hand are inherently shared environments. Corporate data is stored inside large multi-tenanted pools of IT systems and while this can provide substantial economy and scalability, the ability to control, secure and govern corporate data and services is often hindered at best or non-existent at worst.

HFM: What factors should someone consider when choosing between them?
PA: Firstly, consider what IT services are needed and how they are delivered. Both private and public clouds offer a broad range of scalable enterprise IT services, but they can be delivered in differing ways; directly or through a partner, over public or private connections, centrally or distributed, managed or unmanaged. There are advantages and disadvantages to both.

Security, integrity and governance cannot be ignored in the finance industry. With continually growing regulatory and due diligence requirements, it can be challenging to make the move towards public cloud services while private cloud solutions are generally accepted and commonplace within the industry. The security controls, data segregation and access control and protection of systems are readily deliverable in private cloud environments. netConsult holds security as the primary focal point underpinning all of our IT solutions as we believe that maintaining data integrity and control are of critical importance to all businesses. Public clouds often do not provide the means to maintain corporate governance and security of their data and services.

Considering availability, both public and private clouds typically provide services on substantial enterprise IT architectures in top tier datacentres with local and geographical redundancy. Decisions turn to being led by confidence levels taking into account SLAs, incident management, track record, customer service in maintaining and restoring service and retrieval of backup or archive data in the event of an outage or data loss. The latter can be an area where public clouds can be weaker and provide additional challenges, particularly with smaller consumers.

Usability, support and integration can often be considered retrospectively rather than pro-actively. When utilising cloud services, it is essential to appreciate that everyone’s day-to-day interaction with IT services will directly impact business processes. Public cloud providers typically have very fixed and regimented offerings and managing various services from multiple public cloud providers can quickly become costly and ineffective. Private cloud providers will typically manage system integrations and the associated support. For example, netConsult offers an all-encompassing support service alongside our complete solutions with full IT support for clients across their entire IT landscape.

Finally, there is substantial variation in the apparent cost of cloud services; many being substantially economical for...
business of all sizes. However, the value and true cost of cloud services needs to be determined and understood. Public cloud services can have additional hidden costs when it comes to implementing security controls, ineffective and expensive integrations and high support cost from complex maintenance. Private clouds can be more expensive but can offer substantial value as service providers are able to provide integrated security and controls, more cost-effective support, ease of integration with other line of business applications and provide substantial supporting documentation.

HFM: How has hybridisation of these services been created and what advantages does it offer?
PA: Forming a hybrid cloud solution by combining public and private clouds can get more out of public clouds alone; cost-effective service delivery with manageable security controls mitigating some risks of data exposure and complex supportability. While not possible to escape the fundamentals of data storage and security in public clouds, hybridisation can help make up for some of their current shortcomings.

Hybridisation has been achieved by utilising a smaller footprint of private hosted systems coupled with some public cloud services. Adding management, security controls and network visibility moves public clouds more towards the quality of service and security of private clouds whilst leveraging improved economies of scale, reducing maintenance of complex IT systems and enabling additional value added benefits.

netConsult’s hybrid cloud offering enhances Microsoft Office 365 Enterprise Services. We maintain a common security, management and control infrastructure and keep sensitive file data isolated and secured on our private hosted platform. Layering multiple technology suites from different vendors and third-party systems maintains service availability, recoverability and long-term data protection.

HFM: Does cloud technology face a stigma after recent high-profile cases of hacking?
PA: Public cloud technology presents a particularly appealing target for hackers. There are new attack vectors and vulnerabilities in public cloud platforms emerging regularly and with the cross pollination potential, public clouds provide an obvious high-return target for hackers and cyber criminals.

Public cloud technology is relatively young when compared to private cloud technology and like any new technology offering a fundamental change in the practice and delivery of IT services, it has been met with caution from uncertainty. Recent high-profile cases do hamper the cloud’s appeal, however with the amount of high-profile hacking cases spread across the media in relation to more than just cloud services, it more serves to highlight the fundamental requirement of a strong, professional end-to-end security position across all IT services rather than stigmatising one service specifically.

HFM: What are the essential best practices when it comes to cyber security?
PA: The starting point for security systems is to ensure adoption of a professional security position with depth and breadth applying across the whole IT infrastructure. Gaps in controls or security are the first thing that hackers will be looking for.

A layered approach to security is key as no single technology or system will provide sufficient levels of protection. Visibility and intelligence into system and network activity and behaviour using network and event monitoring tools, such as IDS/IPS with SIEM, as simply using legacy perimeter and detection-based tools, such as firewalls, will not provide sufficient levels of security in isolation.

A focus must also be placed into the history of security position to augment point-in-time analytics. A single hack could last over a substantial period of time and visibility needs to be maintained throughout the timeline of the attack, along with coupling this historic visibility with detailed and contextually aware information from next generation security platforms.

HFM: What trends is netConsult seeing from its clients requests? Have these changed in the past year?
PA: Over the last year, netConsult has seen a noticeable change in client service requests and focal points. Firstly, a marked increase in interest in public cloud and hybrid cloud services as the benefits in cost, scalability and accessibility have proven highly attractive, however service levels and enhanced security are expected to be maintained.

Cyber security has been always been a key factor for this industry and netConsult is seeing the trend for security focus continue to increase across our client base, quantified with more awareness and emphasis on data protection; where data is being stored and how it is being managed, who has access to it and how recoverable it is.

HFM: How can cloud technology move forward from here?
PA: Technology trends invariably follow the demands for them. The cost-efficiencies and services that cloud technology can deliver are growing rapidly and are in high demand as they clearly demonstrate a real tangible business benefit. The controls and security of public cloud services have yet to catch up however and are at the moment reliant on either private cloud, in-house systems or even complex system integrations to put the security wrapper around them.

The immediate hurdle for public cloud technology to move forward is very apparent; it must provide a very efficient standard service controlled by the Service Provider, but enable the consumer to customise it and apply their own controls and security to meet their individual requirements. A challenge, certainly, however the demand for it is most definitely there.
REDUCE THE RISK OF CYBER ATTACK

Capital Support’s Cyber Secure services enhance your protection against damaging cyber attacks. Introducing another dimension to your security provisioning, Cyber Secure services have been developed to meet the exacting requirements of regulated financial firms.

- **Cyber Secure Protect and Detect** adds value to your firewall services, offering advanced cyber-attack prevention that enhances visibility and promotes the safe use of systems by users.
- **Cyber Secure SIEM** (Security Information and Event Management) extends the Protect and Detect service with live action and analysis, delivered by security professionals working from a dedicated 24/7 Security Operations Centre.

By engaging with Capital Support, you can significantly reduce the risk of cyber attack to your firm. We’ve been providing highly secure IT services to FCA and U.S. SEC regulated businesses since our inception, and our suite of tailored security services has been developed to meet the needs of the finance sector.

To find out more about us, our services and our experience, please get in touch.

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

THE MOST TRUSTED & RESPECTED IT PROVIDER
Security software providers have an obvious incentive to highlight the risks of cybercrime, are the risks exaggerated?

**Alan Alzfan (AA):** Cyber-crime is a very real and dangerous risk in today’s business world and the financial services community is a prime target based on the fact that these organisations obtain sensitive personal information about their clients, most of who are high-net-worth individuals. The US’ Securities and Exchange Commission (SEC) has identified cyber security as a very important topic, with the Office of Compliance Inspections and Examinations (OCIE) publishing a risk alert on the topic recently based on an OCIE Cybersecurity Examination Initiative conducted in 2014 on broker-dealers and investment advisors.

**Daimon Geopfert (DG):** No, the risk is not exaggerated because it is simply stating reality. If you compare cyber crimes against any other criminal enterprise you’ll see that the opportunity to make money versus the chances of being brought to account by law enforcement (or other criminals) is very low. There is a level of technical knowledge that will currently provide some type of barrier to entry for a large number of criminals, but that barrier is getting lower every month as more powerful but easier to use tools are sold on the underground market.

**HFMWeek (HFM):** Security software providers have an obvious incentive to highlight the risks of cybercrime, are the risks exaggerated?

**Alan Alzfan (AA):** Cyber-crime is a very real and dangerous risk in today’s business world and the financial services community is a prime target based on the fact that these organisations obtain sensitive personal information about their clients, most of who are high-net-worth individuals. The US’ Securities and Exchange Commission (SEC) has identified cyber security as a very important topic, with the Office of Compliance Inspections and Examinations (OCIE) publishing a risk alert on the topic recently based on an OCIE Cybersecurity Examination Initiative conducted in 2014 on broker-dealers and investment advisors.

**Daimon Geopfert (DG):** No, the risk is not exaggerated because it is simply stating reality. If you compare cyber crimes against any other criminal enterprise you’ll see that the opportunity to make money versus the chances of being brought to account by law enforcement (or other criminals) is very low. There is a level of technical knowledge that will currently provide some type of barrier to entry for a large number of criminals, but that barrier is getting lower every month as more powerful but easier to use tools are sold on the underground market.

**HFMWeek (HFM):** Security software providers have an obvious incentive to highlight the risks of cybercrime, are the risks exaggerated?

**Alan Alzfan (AA):** Cyber-crime is a very real and dangerous risk in today’s business world and the financial services community is a prime target based on the fact that these organisations obtain sensitive personal information about their clients, most of who are high-net-worth individuals. The US’ Securities and Exchange Commission (SEC) has identified cyber security as a very important topic, with the Office of Compliance Inspections and Examinations (OCIE) publishing a risk alert on the topic recently based on an OCIE Cybersecurity Examination Initiative conducted in 2014 on broker-dealers and investment advisors.

**Daimon Geopfert (DG):** No, the risk is not exaggerated because it is simply stating reality. If you compare cyber crimes against any other criminal enterprise you’ll see that the opportunity to make money versus the chances of being brought to account by law enforcement (or other criminals) is very low. There is a level of technical knowledge that will currently provide some type of barrier to entry for a large number of criminals, but that barrier is getting lower every month as more powerful but easier to use tools are sold on the underground market.

**HFMWeek (HFM):** Security software providers have an obvious incentive to highlight the risks of cybercrime, are the risks exaggerated?

**Alan Alzfan (AA):** Cyber-crime is a very real and dangerous risk in today’s business world and the financial services community is a prime target based on the fact that these organisations obtain sensitive personal information about their clients, most of who are high-net-worth individuals. The US’ Securities and Exchange Commission (SEC) has identified cyber security as a very important topic, with the Office of Compliance Inspections and Examinations (OCIE) publishing a risk alert on the topic recently based on an OCIE Cybersecurity Examination Initiative conducted in 2014 on broker-dealers and investment advisors.

**Daimon Geopfert (DG):** No, the risk is not exaggerated because it is simply stating reality. If you compare cyber crimes against any other criminal enterprise you’ll see that the opportunity to make money versus the chances of being brought to account by law enforcement (or other criminals) is very low. There is a level of technical knowledge that will currently provide some type of barrier to entry for a large number of criminals, but that barrier is getting lower every month as more powerful but easier to use tools are sold on the underground market.

**HFMWeek (HFM):** Security software providers have an obvious incentive to highlight the risks of cybercrime, are the risks exaggerated?

**Alan Alzfan (AA):** Cyber-crime is a very real and dangerous risk in today’s business world and the financial services community is a prime target based on the fact that these organisations obtain sensitive personal information about their clients, most of who are high-net-worth individuals. The US’ Securities and Exchange Commission (SEC) has identified cyber security as a very important topic, with the Office of Compliance Inspections and Examinations (OCIE) publishing a risk alert on the topic recently based on an OCIE Cybersecurity Examination Initiative conducted in 2014 on broker-dealers and investment advisors.

**Daimon Geopfert (DG):** No, the risk is not exaggerated because it is simply stating reality. If you compare cyber crimes against any other criminal enterprise you’ll see that the opportunity to make money versus the chances of being brought to account by law enforcement (or other criminals) is very low. There is a level of technical knowledge that will currently provide some type of barrier to entry for a large number of criminals, but that barrier is getting lower every month as more powerful but easier to use tools are sold on the underground market.

**HFMWeek (HFM):** Security software providers have an obvious incentive to highlight the risks of cybercrime, are the risks exaggerated?

**Alan Alzfan (AA):** Cyber-crime is a very real and dangerous risk in today’s business world and the financial services community is a prime target based on the fact that these organisations obtain sensitive personal information about their clients, most of who are high-net-worth individuals. The US’ Securities and Exchange Commission (SEC) has identified cyber security as a very important topic, with the Office of Compliance Inspections and Examinations (OCIE) publishing a risk alert on the topic recently based on an OCIE Cybersecurity Examination Initiative conducted in 2014 on broker-dealers and investment advisors.

**Daimon Geopfert (DG):** No, the risk is not exaggerated because it is simply stating reality. If you compare cyber crimes against any other criminal enterprise you’ll see that the opportunity to make money versus the chances of being brought to account by law enforcement (or other criminals) is very low. There is a level of technical knowledge that will currently provide some type of barrier to entry for a large number of criminals, but that barrier is getting lower every month as more powerful but easier to use tools are sold on the underground market.

**HFMWeek (HFM):** Security software providers have an obvious incentive to highlight the risks of cybercrime, are the risks exaggerated?

**Alan Alzfan (AA):** Cyber-crime is a very real and dangerous risk in today’s business world and the financial services community is a prime target based on the fact that these organisations obtain sensitive personal information about their clients, most of who are high-net-worth individuals. The US’ Securities and Exchange Commission (SEC) has identified cyber security as a very important topic, with the Office of Compliance Inspections and Examinations (OCIE) publishing a risk alert on the topic recently based on an OCIE Cybersecurity Examination Initiative conducted in 2014 on broker-dealers and investment advisors.

**Daimon Geopfert (DG):** No, the risk is not exaggerated because it is simply stating reality. If you compare cyber crimes against any other criminal enterprise you’ll see that the opportunity to make money versus the chances of being brought to account by law enforcement (or other criminals) is very low. There is a level of technical knowledge that will currently provide some type of barrier to entry for a large number of criminals, but that barrier is getting lower every month as more powerful but easier to use tools are sold on the underground market.
of the organisation and have a severe impact on the trust of current and future investors.

**HFM:** When it comes to data protection and cyber security audits, what are the key points that all fund managers or risk managers should consider?

**DG:** Many organisations operate under two very dangerous mindsets: that hacking is ‘hard’, and that no hacker would be interested in their organisation because you are the wrong size, industry, etc. Both of these trains of thought are wrong and will get you in trouble in a hurry. First, many aspects of hacking are surprisingly simple but effective such as social engineering. Social engineering is a fancy name for ‘con games’ in which an attacker simply tricks a user into doing something that will allow access to the environment. It only takes a few minutes to create a fake website and send a user an email with a link asking them to visit the website to download updates, vacation photos, audit reports, or any number of false pretences in order to compromise their system. On the second aspect, companies need to understand that the vast majority of breaches were not targeted against any specific organisation. The attackers are simply shooting at anything on the internet hoping that they will be successful. Once their attack works and they gain access they only then know which organisation that got in to, and then they figure out how they will monetise their access. If you are vulnerable somebody will find you, you cannot simply assume you are hiding because you are small.

**AA:** Dealing with cyber security must be made an important part of the overall culture of an organisation. Top management must stress this area just as they stress other important compliance issues. Everyone must constantly be reminded of how one incident can ruin an organisation and how important each person in the organisation is to the program. Like any other compliance program, cyber security must be constantly reviewed and updated. The importance of updating the program cannot be over emphasised as new threats are constantly being deployed and your organisation is constantly being attacked, either directly or indirectly.

**HFM:** What can an organisation do to best prevent against these attacks?

**DG:** The first, and most critical, piece of advice is simply to have a plan. Most organisations do not have any type of incident response plan, and if they do, it is generic with minimal detail. Put in the effort to think through what you’d do if something like this came to pass, and then make sure you exercise that plan so your people don’t have to learn it during the heat of a real event.

Make sure a major part of your plan is pre-arranged relationships with incident response specialists. It is very unlikely that many organisations have full time forensic investigators on staff so it is important to have found them and contracted with them early. In this same mindset, when there is an incident the organisation has to make the very difficult decision to do as little as possible on the network until those forensic experts are on-site. It can be very painful as a responder to have to explain to a client that their initial actions destroyed evidence that was necessary to fully control a breach or answer key questions such as how long it had been occurring.

**AA:** I agree with Daimon. Have a plan. Reach out to your service providers as well as industry colleagues and ask about the actions they are taking in this important area. It may help identify additional areas of consideration for your plan.
The Real Leaders in Global Technology Support

matsco
solutions in technology

Cloud Computing | Project Management | Consulting
Financial Services Implementation Experts

www.matscosolutions.com
GETTING STRONGER TOGETHER

BOB GUILBERT OF EZE CASTLE INTEGRATION EXPLAINS WHY SO MANY FUNDS ARE OPTING FOR CLOUD SOLUTIONS AND HOW THE INDUSTRY CAN WORK TOGETHER TO TACKLE CYBERCRIME

HFMWeek (HFM): What are the security implications of moving to a cloud system?

Bob Guilbert (BG): Firms looking to move to the cloud need to consider which provider is right for them and can service their operational and security needs. A firm needs to consider the security protocols in their office as well as in the cloud and work with someone that covers both sides, including the virtual and physical elements.

It’s also vital that firms understand the ‘response and remedy’ services that cloud providers offer, the quality of which can vary hugely between public and private clouds.

HFM: Can the quality of security offered differ significantly between cloud providers?

BG: Absolutely, which is why IT due diligence is so important. At Eze Castle Integration, we’ve taken a defence-in-depth approach to cloud security starting right at the foundation. We have layers of security all the way through the infrastructure including access controls, continuous security monitoring, and intrusion detection and intrusion prevention systems.

You are only as strong as your last defence. You must have all the right locks on all the right doors and multiple locks on those doors in order to thwart any hacker’s attempts to access your private information. You must also invest in employee training because even the best locks won’t help against many social engineering techniques. These can only be combatted with good due diligence and best practice regarding security awareness training for all staff and senior management.

When evaluating a cloud provider it is also important to understand the security protocols followed within the provider’s corporate infrastructure. At Eze Castle Integration, for example, we’ve invested heavily in our own firm’s security to ensure there aren’t any backdoors to allow a hacker to access the cloud and data of our clients.

HFM: So outsourcing to a cloud platform gives more protection than an in-house product?

BG: I would say so, yes. We are offering enterprise level security, and we have a deep pool of specialists, which can be leveraged when needed for our clients. In-house deployments very often won’t have the same size of staff and also won’t have a budget that allows them to cover all areas of cyber-security to the same degree. Small firms, especially, will never be able to enjoy the scope of security and technological power through their own means that they could by partnering with us.

HFM: Do you predict using cloud services will become the norm in the future?

BG: I think it’s actually reached that stage now. If you look at the number of start-up hedge funds that launch annually, I would say 95%+ of them consider launching on a cloud provider’s platform. One reason for this is the capital expenditure difference between setting up the hardware and software in-house versus selecting an established private cloud provider. Firms get all the benefits of proper management and security to run the environment, and they have predictability in their monthly costs.

HFM: Are established funds, considering their historic investment in in-house IT infrastructure, slower to adopt a cloud solution than start-up funds?

BG: We find there are typically three inflection points where an established firm evaluates a move to the cloud. These are office relocation, technology refresh and adding a new application. A physical move of offices provides an opportunity as firms don’t want to invest in moving and setting up old equipment at a new office. A technology refresh is another logical switching point as firms weigh the costs of doing a whole system upgrade as opposed to moving to the cloud.

In some cases very large funds are still inclined to invest in building their own infrastructure. However, they will look to the private cloud for application hosting. This may be due to the CTO wanting to have the data within the premises of the office. However, Eze Castle Integration has several clients with multi-billion dollar AUMs on our cloud platform. At the highest AUM levels, it often comes down to personal preference and existing investments in internal IT staff and infrastructure.
**HFM: What are ‘Written Information Security Plans’ (WISPs)?**

**BG:** WISPs are plans that cover the administrative and technical safeguards a firm has in place to ensure data is protected. They include details on incident response, remediation and communication procedures should a firm be subject to a cyber-breach. They answer questions such as: have you identified the chief information security officer in the organisation? In the event of a breach what action will you take and what communication paths will you follow?

Having written information security plans is emerging as a requirement for firms. As part of its cyber-security questionnaire, the Security and Exchange Commission (SEC) is asking about WISPs. And investors are increasingly asking to review WISPs as part of their due diligence.

**HFM: So investors have become much more sophisticated on cyber issues then?**

**BG:** Yes, they have. With increasing numbers of successful breaches in the marketplace and more visibility around cyber-security and cyber-crimes, investors are becoming more savvy, aware and concerned.

**HFM: What do you expect from the SEC looking ahead?**

**BG:** The SEC has already said cyber-security is a top priority for them in 2015/16. They are planning to conduct much wider and deeper examinations of funds to ensure they have the best cyber-security practices in place. They also want to see if a fund’s employees have been trained and tested on the firm’s WISP policy.

I believe there is going to be a broader sweep in terms of who is looked at. A number of firms use outsourced functions, and the SEC will soon start to look at these third-party providers in a lot more detail.

“There is still a long way to go, but we all have a common enemy in keeping malicious activity outside of the hedge fund industry, and through effective dialogue between the public and private sectors, we can get stronger together.”

Overall, the security questions being asked by investors and regulators are getting much broader and deeper. Both groups are asking for more details on whether there have been breaches in the past and the process that was taken. Investors are also beginning to ask these details from not only the remedial third party but also all the providers they are using.
**HFMT Technology**

Up-to-the-minute technology news and insight for the global hedge fund space

---

**HFMT Technology** provides the latest news, trend analysis, regulatory updates and comment on the biggest technology issues affecting the hedge fund market, making it an essential business resource for anyone involved with hedge fund technology.

For your complimentary trial visit: www.HFMTTechnology.com
Marcus Lewis is responsible for the continual design, development and review of our managed services catalogue. Lewis is ITIL and Prince II qualified, and his ability to look at the periphery as well as the point of focus is essential to successfully maintaining a large set of services that works in harmony to meet the needs of our customers.

HFMWeek (HFM): What was the motivation behind the creation of this new cyber-security suite?

Marcus Lewis (ML): In April 2014 the SCC published new guidance for cyber-security around the financial sector. What was clear was the level of security consciousness around compliance was quite traditional, such as do you have anti-virus software, is there software in place, etc? We realised there was definitely an opportunity in the IT sector for delivering something more robust and holistic. We therefore began a project to deliver something that was more than just a plug-in application and was focused on offering a comprehensive security service.

HFM: How does this new suite fill the gap in the market for a more substantial cyber-security service? What features will it have?

ML: We came up with three core offerings. This has been collated into part of our new cyber security offering under the banner of ‘Managed Security’. The first is best practice. This doesn’t automatically require new technology, it could just be about making a technology you have more efficient. An example being, have you got high-level password protection for your system? This requires making it company policy to ensure all users have a strong password that is changed regularly.

The second area is consultancy on security and risk management. Our ISO credited chief information security officer carries out a gap analysis and creates a comprehensive report which will highlight the risk that a client may have. From that we can then discuss these risks with the clients and clarify what that risk means to them; this is vital because an exposure can be highly important for one company to mitigate but not so key for another.

For example, if your website is just a brochure site with only your own contact information included, that is very different to a website that may request sensitive and confidential information from its users. The consequences of a successful hacking attempt on the first website is marginal compared to the second. Therefore your investment in security for either type of site can be very different. While our clients choose which services they subscribe to, it is our responsibility to give the best possible advice so that they understand the risks to make the right business decisions.

HFM: What guidelines do you use for your own best practice standards?

ML: We use ISO 27001:2013 standard and the government Cyber Essentials and Cyber Essentials Plus as guidance along with security reference sites eg, NIST and the Centre of Internet Security (CIS) tools, which has server and desktop benchmarking that acts as a good yardstick for us. For example the CIS has 245 separate recommendations on how to ‘harden’ a server, which we can use as a template. We also take on advice from our security partners and all this combines to give us a solid foundation for our security procedures.

HFM: What happens if you find your client’s current protection software is inadequate?

ML: If our report concludes that new security devices are recommended then we move onto the third area of our service where we have several products that come as part of our suite offering. First is Cyber Secure Protect and Detect. This adds a next generation firewall which scans data as it enters and leaves the network. It scans for viruses and rogue activity as well as web and application filtering. Examples of app filters could be that we can manipulate the settings so that users who want to access Dropbox or Facebook can download data but cannot upload it, meaning no data can leak out that way.

We can adapt the system further so that most users are unable to access or upload to Facebook except the specific members of the marketing department, who have legitimate, work-related reasons to do so.

Historically, firewalls could be considered as an open or shut door. It looks at an email’s details but not what is actually in it. Next-generation firewalls, like ours, will scan the actual contents to the point where we can set it to look for bank account numbers...
actual contents to the point where we can set it to look for things like a specific set of bank account numbers that the clients is especially keen to avoid leaking.

In addition to the firewall we also offer a SIEM service (security information and event management). This service monitors event logs for all the data moving around your system on all devices. Several million entries can be created per day, which would be impossible for staff to effectively study for possible discrepancies. Therefore the SIEM service uses a correlation engine that follows a predefined set of rules to analyse the information for things such as multiple failed entry requests from a foreign IP address.

This service is very sophisticated and can even recognise when several smaller logs that wouldn’t raise concern by themselves actually form a pattern that is suspicious. Monitoring the events and alerts using our manned 24/7 Security Operations Centre, we alert clients of potential threats and actions they should take to eradicate potential weaknesses in their network.

HFM: Does your security advice revolve exclusively around the cyber element?
ML: No, our security advice is around protecting information assets and is not just about technology; it is also about people and processes. Risk management can’t just be about IT, it’s got to include the bigger picture.

We ask our clients what is the most business critical asset and then look at the controls, for example, their policy on leaving data around the office, what’s the entry policy for your building? What’s your HR policy regarding new or leaving staff? Do you allow data to leave the building and is it monitored? All these things might have an IT solution but require a HR document which staff can follow.

We do also have some software available that creates a secure method for staff to access and send data remotely if there is a significant exposure to data loss or manipulation.

HFM: The technology industry is incredibly fast-paced. How do you ensure any new offerings are future-proof, or is this impossible?
ML: In part the on-going success of our product is down to people and processes. You can have the best locks in the world but if you leave the front door wide open they aren’t going to help. That’s why personnel training and education is so important.

No system is future-proof as technology is constantly advancing and so is the sophistication of cyber criminals.

With regard to the software we use, there are a few things we can do to stay ahead of the enemy. Our firewall is updated daily in order to keep abreast of the forms of attack that might come. Everything has to come through our firewall so if we know what an attack looks like we can always stop it.

On the hardware side, we can incorporate any new technology into our SIEM engine and create new rules around it. We can’t know everything all the time but considerable investment, by us and our technology partners, go into making sure what we don’t know now we will soon and this will continue in the future.
Your data is attacked hundreds of times a day. Do you still like your odds?

Power comes from being understood.

It’s no longer a question of if you’ll suffer a cyber breach, it’s a question of when. How quickly you detect and how effectively you respond to and contain that breach could shape the future of your business.

McGladrey understands. Over the last 50 years, McGladrey has served more than 1,500 investment companies. We understand more than cyber security—we understand it within the context of your complex operational, reporting and compliance environment.

Want to improve your odds? Watch http://mcgladrey.com/hedgefund and experience the power of being understood.
Options is the leading managed service and IT infrastructure products provider to the global financial services sector. Founded in 1993, the company began life as a hedge fund technology services provider. More than a decade ago, the company made a strategic decision to become the first provider to offer cloud services to the financial sector. Today, more than 150 firms globally leverage the Options platform, including the leading global investment banks, hedge funds, funds of funds, private equity houses and exchanges.

HFMWeek (HFM): There are now several IT service providers to the financial sector. What makes Options’ offering stand out?

John Bryant (JB): From day one we set out to deliver bullet proof, ‘investment bank’ grade infrastructure and service, leveraging a global technology platform. Having such a clear vision has allowed us to stand out on multiple fronts. We have a global team and global infrastructure, allowing our customers with global operations to work with a single vendor; most of our competitors, by comparison, are focused in one region or service. Our focus on building the platform to exacting standards means that many of the features that are expensive add-ons with competitors are base features with Options. Examples include DR, replication and hot-redundancy, daily backups to tape, carrier diversity and in-region data centre resiliency. Feedback from customers is that the majority of competitors either treat these fundamental features as up-sell or in some cases don’t offer them at all. In London, for instance, a number of firms base all their services from data centres in the Thames flood plain – a design that would be immediately thrown out in any top tier firm.

Another thing that sets Options apart is the focus on building security and transparency into our processes and procedures. Options has been leading the market in this regard for many years. We were among the first service provider of our kind to be SOC accredited (since it was first introduced in 2011) and we’ve made our cyber-security policies and best practice recommendations open and available for download online. We have been making a substantial investment in the leading security related technologies for a
number of years now and will continue to do so. Penetration tests are a case in point, both Options and our leading customers do regular pen tests and we are happy to share our results with customers and prospects.

HFM: Options has a global market presence. Which areas are most sophisticated in their service demands and which are more reluctant to invest in cyber-security?

JB: Had you asked me that question two years ago, my answer would have been that our US and UK institutional client base was much more sophisticated in terms of security demands – with SLAs stipulating schedules for security patching, server reboots, login audits, penetration tests, intrusion prevention log reviews, etc. Historically, the adoption of fundamental security best practices such as password expiry or complexity was an unremarkable hurdle for some hedge fund COOs. However, in the last 18 months, with increased scrutiny both from regulators and investors, hedge funds display an increasing awareness of the risks posed by a laissez-faire attitude to security. Many no longer see it as a burden, instead using their firm’s security policies and infrastructure as a positive to attract institutional investment.

HFM: What are the must-have features of a cyber-security offering in today’s fund industry?

JB: Any security offering in this space should combine both the need to actively scrutinise each layer of your IT architecture as a point of potential weakness with the need for service uptime and operational flexibility.

As an example, our security offering combines best practice security building blocks (e.g., IPS-enabled firewalls, access-lists, platform agnostic anti-spam/malware and vulnerability scanning tools) one might expect, together with automation and the operational rigour to check all security-related data for signs of unwanted behaviour, and review security bulletins for the latest vulnerabilities exploited in the wild. Without the foundation of those processes and the efficiency of that automation these tools would fail to reach the full potential of our investment in them.

Although the zeitgeist may today be around mobile malware and anti-DoS appliances, it pays to do the age old fundamentals well – audit your systems regularly, ensure your data is backed up, log all activity, reboot PCs and servers so they get the latest security patches, and reduce the potential attack entry points (disable portable media, use web filtering, filter spam).

Lastly, do not overlook the benefits of end user IT security training and awareness. Your cyber-security infrastructure is only half the story.

HFM: When it comes to sensitive data management and protection, are managers sufficiently aware of the risks posed by cyber-attacks?

JB: The order of magnitude increase in media attention given to the topic of cyber risk over the past year alone has certainly heightened the awareness of the business community at large, and broadly we do see an appropriate level of awareness to the wider issues at work here. The question is are those managers committed to budgeting for and taking the necessary actions to address them, and here again we see a positive and accelerating trend.

HFM: With cyber-attacks becoming more and more common as well are varied in their methods, how can Options offer security to its clients?

JB: Options has invested significantly in our infrastructure in order to meet the increasing security demands service providers are facing in this space. All of the components we touched on above are key building blocks that form our security offering to clients. We’ve built and matured the Options global private network over the past 10 years, enabling best-in-class information security for our clients. While other vendors in the space continue to use VPNs, customers leveraging the Options platform can harness a fully resilient and secure global platform with high bandwidth and low latency.

“OPTIONS HAS INVESTED SIGNIFICANTLY IN OUR INFRASTRUCTURE IN ORDER TO MEET THE INCREASING SECURITY DEMANDS SERVICE PROVIDERS ARE FACING IN THIS SPACE”

In the past 12 months alone we have invested in a number of security and compliance products to enhance our security offering including Active Directory auditing, Windows file system auditing, BYOD management, and a web filtering platform refresh, to name but a few. All of these additions come at no extra cost – they are bundled within the service charge.

HFM: Which aspects of your offering are you looking to develop in the next year?

JB: One of the latest initiatives we have committed to is to use Splunk as our enterprise SIEM product. We already use the Splunk platform in our day-to-day IT operations. Over the next few months we will bring all relevant security data such as firewall, web filtering, IPS and antivirus logs together into a single information repository. The new platform will also replace our current vulnerability scanning tool.

This represents a huge leap forward in our capabilities in this space, allowing us to react much more swiftly to detect new threats, diagnose anomalous behaviour, conduct forensic investigations and perform security analysis in real time.

Additionally, we have recently introduced monthly management packs that report on key security metrics in real time to provide clients with the transparency they need. While still in beta, these are due to be rolled out to our client base in due course.
Economic cyber crime does not discriminate. It is truly global. No industry or organisation is immune.

The fallout isn’t just the direct costs. Economic cyber crime seriously damages brands, tarnishes reputations beyond repair and impacts market share. As society becomes less tolerant of unethical behaviour, businesses need to make sure they are building – and keeping – trust.

Against a backdrop of data loss, IP theft and financial fraud, ENCODE’s Extrusion Testing™ and Cyber Readiness Assessment service, a simulated cyber attack providing you with the insight you need to address the threats that matter, combined with the Cyber Operation and Intelligence service, which delivers the visibility, early detection and adaptive response you need to protect your organisation against obscure, targeted cyber attacks.

Take control.

+44 (0)207 406 7535
www.encodegroup.com

Encode Group, 5 Chancery Lane, London WC2A 1LG, UK
WARREN FINKEL, OF ACE IT, EXPLAINS WHY CYBER-SECURITY MUST INCLUDE
A TOP-DOWN APPROACH TO SECURITY AWARENESS

HFM: What is ACE IT Solutions’ approach to cybersecurity and its main principles?
Warren Finkel (WF): Our cyber-security solutions are tailored to help firms be proactive and meet compliance requirements. The fact is, your firm will get hacked; it’s no longer a matter of if but when.

The key to minimising risk is using threat intelligence to get ahead of hackers. With up-to-date, customised intelligence about current and future threats, and a deep understanding of how well your security strategy stands up to these threats, you can better manage your defences while reducing risk and making smarter investments. Threat intelligence also help you understand which threats are applicable to your businesses. A one-size-fits-all approach does not work as well as a customised approach to taming your firm’s threat landscape.

This includes security awareness training to help employees understand how they put their firm at risk, training them about cyber-security best practices and how to recognise phishing emails – a primary entry point for hackers.

HFM: ACE IT Solutions partnered with IBM, which was rated number one by Gartner for threat intelligence. What is ‘threat intelligence’ and how is it employed against cybercrime?
WF: The more information you have about the threats that are out there, the better prepared firms can be to deal with the risks. Threat intelligence can be used to defend against attacks, but it is incredibly useful for helping recognise an attack and dealing with it. Think about it like this: we know company A, B, and C got hacked and this is how it happened. How can we use that information to mitigate a cyber-attack on our own firm?

Even the US government is getting behind this approach. It recently passed a bill that would push companies to share information about security breaches. This is important because businesses can no longer fight the bad guys individually. We must use the compiled threat intelligence from the whole industry to fight them.

HFM: There is a clear need to educate your clients’ staff to employ best practice and avoid a breach through phishing techniques, etc. How do you approach this?
WF: We are doing a lot of employee training on safe internet use, including phishing exercises to help them recognise phishing emails. Teaching employees to be aware of an organisation’s security requirements can be one of the most effective ways to enhance the company’s overall security posture. Employees are a key link in the security of a business’ technology infrastructure and company data. Without end-user training on security best practices and policies, it is impossible to secure your information resources or ensure data privacy. The effort to create a ‘security aware culture’ must include everyone in the company. Additionally, end-user training on security best practices and privacy awareness is essential to any organisation’s compliance and risk management initiatives.

We also educate people on the weaknesses of certain cloud apps and ensuring employees don’t have admin access that allows them to download applications and access back-office functions.

As an IBM partner we can offer our clients access to its security operation centres and the X-Force threat intelligence team, but if you don’t have the basics of an educated and aware staff then it won’t help prevent a breach.

HFM: What is the most important feature of your staff education process?
WF: The key is that change is driven from the top. We often speak to IT staff from a fund who are obviously very aware of the dangers of cyber-attacks and how to avoid a breach but more often than not when I speak to CFOs or CEOs they don’t even know what basic controls their fund has in place. Senior management must be made aware and then drive best practice procedures. Information security policies, incident response plans are also critical to a cyber-security programme. The SEC is now requiring these plans to be in place and that you have a penetration test.

Ultimately, we have all the services a client could want and we understand the SEC’s requirements but the best cyber-defence mechanism has to start internally by creating a culture of awareness and training employees to comply with laws, regulations and policies to reduce the risk of exposure.
EVERY WEEK YOU WILL RECEIVE

More exclusive stories than any other hedge fund publication
All the latest searches and investment news
Exclusive data on launches and performance
Investment strategy analysis
Topical comment from leading industry figures
Exclusive research surveys
Regulatory developments
People on the move

As a subscriber, you will also receive full registration to www.hfmweek.com, where you can access:

Daily updated performance data
Exclusive research
Daily news alerts
Industry events information
Service directory listings and much more...

FOR MORE INFORMATION PLEASE CONTACT
The Membership Team at +44 (0)207 832 6511 OR email membership@hfmweek.com
OR VISIT HFMWEEK.COM FOR DETAILS
THE ATTACK HAS EVOLVED, HAVE YOU?

DAN BONNET, SALES DIRECTOR, DELL SECUREWORKS, TALKS TO HFMWEEK ABOUT THE MUST HAVE FEATURES OF A CYBER-SECURITY SERVICE PROVIDER

The US Security and Exchange Commission (SEC) has provided cyber security risk guidance for investment management firms. Hedge fund firms are spending more for cyber security to align with the guidance but are missing many opportunities to optimally secure their networks. The focus should be on security. Once that is taken care of, the SEC recommendations will automatically fall into place.

If you have not yet focused on cyber security, you are not alone. In the SANS Institute report (Securing the Human 2015 Security Awareness), the cyber security institute discovered that half of the organisations surveyed currently do not have an awareness programme or have an immature programme that is solely focused on compliance. Focusing on compliance gives organisations a stronger security posture but could leave out important processes in securing a network. Most organisations have put a few protective and detective security devices, software products and security policies in place, and think they are secure. However, if you are not looking beyond your network and into your endpoints, employees and processes, then client trust and reputation is at risk.

A recent survey of global institutional investors by KPMG found that 79% of investors would be discouraged from investing in a business that has been hacked. Security today is not based on devices alone. It is based on a combination of people, process and technology.

SECURITY TODAY IS NOT BASED ON DEVICES ALONE. IT IS BASED ON A COMBINATION OF PEOPLE, PROCESS AND TECHNOLOGY

Before you have been breached, you should have already thought about and have answered the following questions:

- Who is going to manage the threats that are discovered?
- Who is going to assess what damage has been done thus far?
- Will this person have the tools and a database of billions of threats and threat activities, all necessary to analyse the suspicious activity to determine exactly what malware is in your network?
- Who is going to find out where in your network the threats are and how the intruders entered?
- Who is going to be able to remove the threat?

Before investing in any cyber security infrastructure, answer those questions. If you’ve spent thousands of dollars on a device that is not being patched, managed, and configured consistently, your firm’s assets aren’t properly protected. Just as a hedge fund needs a fund manager, hedge funds need security experts to help them manage their networks.

At a hedge fund management seminar in September 2014, the SEC said, “Compliance policies and procedures must be specifically tailored to your firm’s advisory business, and should evolve and grow with your business... It is crucial that policies and procedures be reviewed and updated as your business changes, as regulations change, and as new guidance is issued.”

Those are principles your cyber security strategy should encompass. As your business changes, so does your network, which is why you need operational and technical controls to protect it. However, you can’t decide what controls to implement without knowing where your network is at risk. So a risk assessment should be one of the first steps you take when analysing your security. This will help you assess risk based on probability, impact and cost.

You also should conduct a vulnerability assessment to
discover current weaknesses in your network. An automated scanner may scan for firewall configuration weaknesses, open ports and default login credentials. However, an expert is needed to delve deeper into your network to manually scan it in order to find errors that automated tools often make and to review security policies and logs, and personnel processes to discover other weaknesses.

You should next conduct a penetration test, or pen test. By simulating an attack without harming your network, this test assesses how well your deployed security controls are working and to what extent an attacker could cause damage.

One of the biggest problems organisations face is they don’t know when they are being targeted or when they have been compromised. In the 2014 Ponemon research report *The Year of the Megabreach*, it took one-third of the organisations represented in this research two or more years after an incident to discover they had been breached. 20% were unable to determine when the breach was discovered, making it difficult to determine the extent of the breach and the root cause. Threat intelligence and 24-hour monitoring can help you know when your adversaries are targeting you and how to stop them before they reach your assets.

Security professionals who have the know-how and experience can help you create a long-term security strategy to develop and maintain a secure network. A vendor that has knowledge of only some network security operations but does not have its own threat database and incident response team won’t have all the knowledge that is needed to combat threats, and could leave you with gaps in your cyber security programme.

To secure your client database, trading algorithms, proprietary trading secrets, strategies and business processes, you need the utmost security. Experts who work in security full time need to do many things in order to truly understand the tactics, techniques and procedures threat actors use.

The best security experts for hedge funds and financial services should provide the following services:

- Monitor the networks of more than 1,000 financial services clients to have firsthand knowledge of their targeted attacks
- Can provide you with knowledge of threat actors who are targeting you so you can stop them before they reach your assets
- Have a personal global view of the threat landscape from monitoring thousands of networks around the world to see exactly the type of threats that are out there and to advise you what you need to do to protect yourself
- Monitor the threat underground to understand the attackers and catch threats before they hit you
- Be able to continually manage, configure and provide updates to your protective devices so that they actually block the threats as they were designed to do
- Provide countermeasures for the most recent threats
- Conduct incident response engagements, to provide insider knowledge as to who the threat actors are and how they work
- Consistently analyse malware and its activities so when you get strange activity in your network, they can identify it and remove it.
**Capital Support Limited**, Nigel Brooks, Managing Partner // T: +44(0)20 7658 1250  Carrie Sauders, Executive Director of Sales // T: +44 (0)120 7658 1250

Capital Support specialises in implementing and supporting end-to-end IT solutions for a large portfolio of global finance sector customers. The company ethos is to make IT simple for its customers, providing intelligent designed tailored solutions that span the breadth of regulated firms’ requirements. Capital Support’s vision is to be the most trusted and respected managed IT services provider. 2015 is seeing a continued rise in the number of cyber-attacks suffered by businesses across all sectors. Finance sector firms are amongst the most prized targets for cyber criminals. Capital Support’s managed security services provide peace-of-mind to businesses, investors and regulators.

**Dell SecureWorks**, Dan Bonnet, Sales Director // dbonnet@secureworks.com // T: +1 404 486 9478

Dell Inc. listens to clients and delivers innovative technology and services that give them the power to do more. Recognised as an industry leader by top analysts, Dell SecureWorks provides world-class information security services to help organisations of all sizes, including asset management firms, protect their IT assets comply with regulations and reduce security costs.

**eSentire**, Mark Sangster, VP of Marketing // Tel: +1 512 651 2200 // 1 Penn Plaza, Suite 4501, New York, NY 10129 // www.esentire.com

eSentire® is the leader in Active Threat Protection solutions and services, the most comprehensive way to defend enterprises from advanced and never-before-seen cyber threats. eSentire’s flagship offering, Network Interceptor, challenges legacy security approaches, combining behaviour-based analytics, immediate mitigation and actionable intelligence on a 24x6x365 basis. The company’s dedicated team of security experts continuously monitors customer networks to detect and block cyber attacks in real-time. Protecting more than $2tn in combined assets, eSentire is the trusted choice for security decision-makers in financial services. In 2014 eSentire was named Best Security Service Winner at IFM’s US Services Awards. For more information visit www.esentire.com and follow @eSentire.

**Eze Castle Integration**, Dean Hill, Executive Director // +44 (0)207 071 6835// Simon Eyre, Director of Services // +44 (0)207 071 6835

Interpark House, 7 Down Street, London, W1J 7AJ, email: www.eci.com

Eze Castle Integration is the leading provider of IT services and private cloud services to over 650 alternative investment firms worldwide, including more than 100 firms with $5 billion or more in assets under management. Since 1999, Eze Castle Integration has developed financial vertical-specific IT solutions including infrastructure design and management (both in our Eze Private Cloud and on premise), telecommunications, business continuity planning and disaster recovery, archiving, storage, and internet services. These solutions are complemented by a broad service organisation that delivers outsourced IT support, including a 24x6 help desk, project and technology management services, consulting services and more. Eze Castle has presence in major financial centres including 8 US offices, a Singapore office, and a Hong Kong office in addition to its London office.

**Matsco Solutions Ltd**, Jim Serpi, Director of Global Operations // London +44 (0)20 7821 4950 // Hong Kong +852 8101 8418 // Singapore +65 6300 1090 // New York +1 866 446 9226 // Beijing +86 400 120 2782 // email: jsrpi@matscosolutions.com // Gilbert El-Zmetr, Director of Asian Operations, Hong Kong +852 3973 8900 // email: j.el-zmetr@matscosolutions.com

Matsco Solutions is a leading IT services and support company founded in 2002 with offices in London, New York, Connecticut, California, Hong Kong, Singapore and Beijing. Specialising in the financial services industry, Matsco Solutions provides IT services and support for a full range of business operations and requirements from sole traders, small and medium size enterprises (SMES) and large multi-nationals. We provide 24/7 support and project solutions to a wide range of businesses across the globe. We specialise in company start-up services, support and monitoring, business consulting, private cloud services, IT engineering and design, outsourcing, project management, start-up projects and implementations.

**McGladrey**, Alan D. Alzfan, Partner, Financial Services Practice - North America // T: +1 212-372-5380 // alan.alzfan@mcgladrey.com

Lynne Well, Partner, Financial Services Practice, N America // T: +1 322 634 4668 // lynne.well@mcgladrey.com

With more than 50 years of experience serving the financial services community in key financial hubs, McGladrey professionals help organizations navigate complex reporting, governance and regulatory issues to achieve their business objectives. Based on the knowledge that comes from serving alternative investment companies, investment advisors, investment partnerships/hedge funds, private equity funds, business development companies, mutual funds, broker-dealers and futures commission merchants, we understand the complex operational, financial reporting and compliance issues facing the industry. We provide industry insight, advice and solutions to financial services organizations across the country and around the world. That’s what you can expect from McGladrey. Experience the Power of Being Understood™

**netConsult Ltd**, Level 3, 75 Wells Street, London W1T 3OH // www.netconsult.co.uk // David Mansfield, CEO // T: +44 (0)20 71003310 // dmansfield@netconsult.co.uk // Laura Zverko, commercial director // T: +44 (0)20 71003310 // lzverko@netconsult.co.uk

Established in 2002, netConsult is an award winning provider of managed IT Services to the global alternative investment industry. We aim to provide a high level of technical expertise to our clients combined with a dedication to customer service. Our ethos is based upon designing secure IT platforms which are manageable over the long term. We are a trusted technology provider to a large portfolio of clients ranging from small start ups to large global funds. netConsult provides a bespoke service to its clients and provides a full suite of IT services including cloud services, outsourced IT BDI virtual CTO and IT security.

---

**capital**

**Dell**

**SecureWorks**

**eSentire**

**Eze Castle Integration**

**Matsco Solutions Ltd**

**McGladrey**

**netConsult Ltd**
Cybercriminals are watching
Regulators are coming
Clients are asking
Are You Prepared?

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

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

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

BOSTON | CHICAGO | DALLAS | HONG KONG | LONDON | LOS ANGELES | MINNEAPOLIS
NEW YORK | SAN FRANCISCO | SINGAPORE | STAMFORD

Speak to netConsult on 020 7100 3310

Established in 2002, netConsult is an award winning provider of managed IT Services to the global alternative investment industry.

We aim to provide a high level of technical expertise to our clients combined with a dedication to customer service. Our ethos is based upon designing secure IT platforms which are manageable over the long term.

We are a trusted technology provider to a large portfolio of clients ranging from small start ups to large global funds. netConsult provides a bespoke service to its clients and provides a full suite of IT services including Cloud Services, Outsourced IT, BCP, Virtual CTO and IT Security. For more information visit www.netconsult.co.uk