Lawson Conner Regulatory Update

Cyber Security for Asset Managers

15 December 2016

Issue: Q4 2016

Contact: +44 (0)203 696 2568

Andrew Frost, Director Investment Management Solutions (afrost@lawsonconner.com)

Gerhard Grueter, Managing Director (ggrueter@lawsonconner.com)

Jurgen Gebhard, Managing Director (jgebhard@lawsonconner.com)

Steve Robertson, COO (srobertson@lawsonconner.com)

Ronnie Menassa, IT/ Infrastructure (rmenassa@lawsonconner.com)

Please refer to the Disclaimer at the end of the newsletter for further reference.

Further information:

www.lawsonconner.com

The Risk from Cyber Security Threats

As a result of technological advancements, the use of mobile and cloud-based platforms has increased tremendously. These trends force financial services firms to review their face with heightened requirements to protect their digital assets, such as private information, board minutes, company business plans and strategies, financial deposits and trading algorithms.

Therefore, it is crucial to embrace the best technology and expertise to prevent any theft or damage before it happens. However, it has also been highlighted by cyber security experts that recruiting the right people with the right skills and knowledge of the processes is as important as investing into technology since employees can act as the organization's first line of defence by working within common frameworks.

Why Asset Managers are threatened?

- The Financial Services industry is one of the most targeted industries by cyber criminals.
- Asset Managers not only control valuable financial assets but also large amount of data is handled electronically.
- Due to regulatory changes companies regularly need to assess whether new policies along with new processes and procedures need to be implemented.
- To date, the culture of asset management firms have not forced awareness and consideration of potential threats of cyber attacks.

How to Reduce the Risk of an Attack?

- **Employees' Awareness**

  First of all, it is essential to create a cyber risk aware culture, driven from the top down. It can be achieved by providing security awareness training on basis to employees, followed up with periodic refreshers to enable them to identify suspicious activities more quickly. Focusing on areas such as password security and composition, identification of phony emails, data protection in public places, effective use of social media and cyber attack methods can make it more difficult for attackers to gain access to confidential information.

- **Asset Inventory**

  Another crucial part of cyber-security is how data is handled and who has access to it. Firms need to keep records of access rights to electronic data to ensure they are backed up and traceable when employees leave the firm.

- **Risk Strategy**

  A cyber risk strategy needs to be implemented at the executive level as an integral part of the company strategy. It is crucial that risk officers along with IT specialists get support from the management team. The management team is responsible for the governance of the cyber security strategy.

- **Policies and Procedures**

  Implementing cyber-security policies and procedures can provide step-by-step instructions for achieving consistent approach in day-to-day technology operations, including responsibilities, tasks, application and process.

- **Technological Updates**

  Technological innovations have significantly increased the number of access points to data (i.e. email, mobile devices, websites, tablets) resulting in more loopholes that hackers can exploit. Therefore, firms need to regularly update to new detection and monitoring software.

- **Reporting**

  Implementing an incident/problem tracking and reporting system can help assess the firm's current threats, risks and actual breaches by storing the type of attack, tools utilised by the attacker, amount of time it took to detect the breach, processes impacted by the attack, number of impacted users and financial damage of the attack. Moreover, trend analysis can be performed which helps to identify potential attack patterns as well as the types of threats that the organisation is more likely to get. It also helps to report any attacks to regulatory organisations when required.

- **Information Sharing**

  Firms need to keep the lines of communication open and share information in industry bodies to work together to identify and tackle attacks. Also, information on new threats and vulnerabilities can be also obtained from other sources such as industry events, peer discussion groups, newsgroups and security vendors.

Please, ask one of our cyber security experts for advice.

About Lawson Conner

Lawson Conner is an award-winning provider of compliance & regulatory infrastructure.

Lawson Conner offers customised solutions in the areas of Fund Structuring, Outsourced Compliance, Global Regulatory Infrastructure, Fund Distribution, Regulatory Hosting, Cyber Security, Appointed Representative Services and ManCo Services.

Solving our clients' most complex regulatory and compliance challenges is not only a fundamental goal but it is the reason why we exist. As a reliable and trusted partner, we create long term value by working with passion, expertise and unparalleled commitment to the industry and our clients.

How to get in touch

London (HQ)
134 Buckingham Palace Road, London, SW1W 9SA United Kingdom
P: +44 207 305 5810
E: afrost@lawsonconner.com

Singapore (Asia Hub)
Marina Bay Financial Centre, Tower 2, Level 39 10 Marina Boulevard, 018983, Singapore
P: +65 31 637000
E:jgebhard@lawsonconner.com

New York
30 Wall Street 8th Floor New York, NY 10005 United States of America
P: +1 646 5689965
E:ggrueter@lawsonconner.com

Boston
Ten Post Office Square, 8th Floor, Boston, MA 02109 United States of America
P: +1 617 9399599
E:boston@lawsonconner.com

Hong Kong
Time Square Tower 2, 1 Matheson Street Causeway Bay, Hong Kong
P: +852 5 8083812
E:jgebhard@lawsonconner.com

Sources

https://www.ipe.com/reports/special-reports/technology-sector/cyber-security-in-asset-management/10007766.fullarticle

http://www.investmentweek.co.uk/investment-week/opinion/2427619/why-asset-management-must-learn-lessons-from-other-sectors-on-cybercrime#

https://irmsecurity.com/blog/5-key-cyber-risks-facing-asset-management-firms/

http://www.ey.com/Publication/vwLUAssets/EY-10_security_considerations_for_asset_management/$FILE/EY_Cyberrisk.pdf

https://www.fca.org.uk/news/speeches/our-approach-cyber-security-financial-services-firms

DISCLAIMER

Any research ("Research") published is to be seen as general in nature and has been prepared solely for informational purposes and is not an offer to buy or sell, or a solicitation of an offer to buy or sell any interest in certain any investment products or any asset classes mentioned herein or any other security or instrument or to participate in any investment strategy. No undertaking, representation, warranty or other assurance is given, and none should be implied, as to, and no reliance should be placed on, the accuracy, completeness or fairness of the Research or opinions contained in any Research provided by Lawson Conner. Lawson Conner's opinions and estimates constitute Lawson Conner's judgment and should be regarded as indicative, preliminary, strictly non-binding and for illustrative purposes only. The information contained in any Research publication has not been verified by Lawson Conner, not any of its associates, partners or affiliates.

The circulation of Research and the offering of interests as described in this website may be restricted in certain jurisdictions. The contents of this website do not constitute an offer, promotion or solicitation to any person in any jurisdiction in which such offer, promotion or solicitation is not authorised, or to any person to whom it would be unlawful to make such offer, promotion or solicitation. This Research and any information is directed only at persons in the United Kingdom who are Relevant Persons and must not be acted on or relied on by anyone else in or outside the United Kingdom.

The information contained within all Research has been prepared in good faith, based upon publicly available information originating from sources believed to be accurate, and which are attributed where relevant. Lawson Conner has not verified that information, and so makes no representation, guarantee or warranty, express or implied, as to the accuracy or completeness of the information relied upon. No undertaking, representation, warranty or other assurance is given, and none should be implied, as to, and no reliance should be placed on, the accuracy, completeness or fairness of the information or opinions contained in this document (together the "Document"). The information contained in the Document has not been verified by Lawson Conner, not any of its