Cyber security – Asset management industry

Asset/fund management crown jewels – Where are the attractions?

Targets across the asset/fund management value-chain

Portfolio management	• Client portfolios • Proprietary fund information
Fund administrator	• Fund's accounting and financial records
Custodian/ bank	• Fund's assets and information • Fund strategy
Fund registrar	• Register of shareholders
Broker trading	• Personal and financial information of shareholders

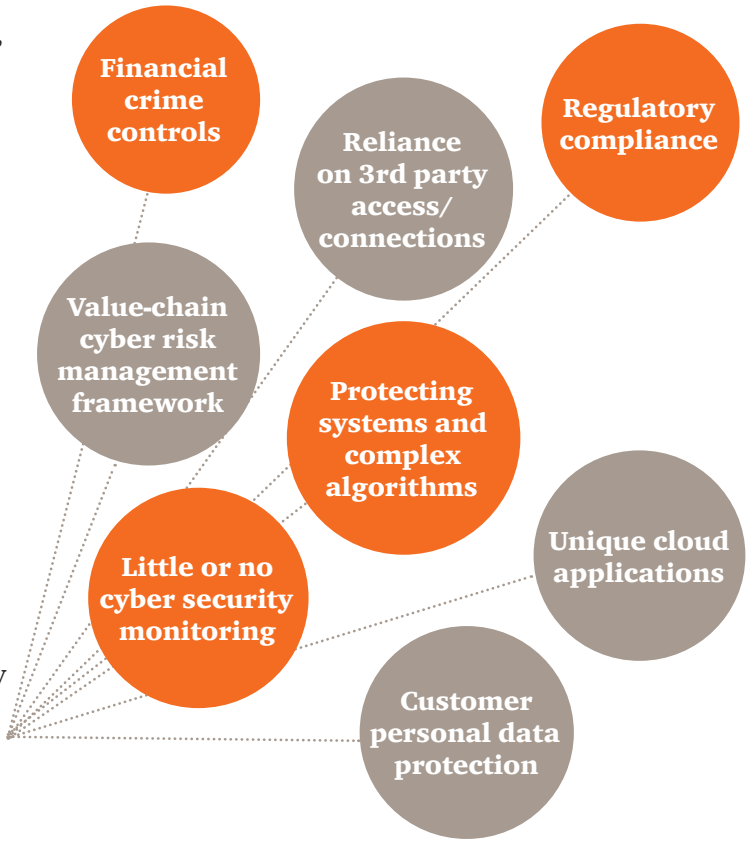
Unique cyber risk challanges for the asset management industry

The asset management industry faces some unique challenges – it holds a tremendous amount of capital, significantly sensitive proprietary information, and market sensitive algorithms, but they are typically boutique operations often with very basic IT and functions.

With increased digital connectivity across the asset management value-chain, security risks and points of vulnerability can go unmanaged and undetected, leaving the door open for cyber criminals to exploit – example if a broker trader was compromised, in addition to the theft of sensitive customer data, they could infiltrate other parts of the value chain causing disruption and negative impact on fund values.

The potential risk of damage to your business operations, distribution channels, investor and market confidence, and the consequential financial losses is significant.

Understanding and assessing your own cyber security posture and dealing with the unique challenges applicable to the asset management sector is critical:



The reality: Impact to business

Making headlines – you don't want to be next.

Cyber attacks on fund management firms have increased, so have the methods of entry into these systems allowing various avenues of compromise into the control systems environment. Attack vectors historically only seen in corporate networks are now a concern for fund management systems as well.

"Huge data leak at largest US bond issuer"

A misconfiguration in a company web server had exposed coutless customer account numbers, balances and other sensitive data

KrebsOnSecurity, Oct 2014

"US Govt warns hedge funds pose cyber risks"

Fund managers are weak link in financial system's defences against hackers and terrorists

Financial Times, May 2015

"Cybersecurity firm says large hedge fund attacked"

Cyber criminals installed a malicious computer program on ther servers of a large hedge fund, crippling its high-speed trading strategy and sending information about its trades to unknown offsite computer

CNBC, June 2014

"Fidelity attacked by JPMorgan hackers, no data stolen"

Fidelity Investments was among 13 financial institutions attacked by hackers who are believed to have been responsible for a breach at JPMorgan Chase

Reuters, Oct 2014

"American Funds warns on 'Heartbleed' bug"

American Funds said approximately 825,000 clients could have had their passwords revealed

Financial Times, April 2014

"Zevin Asset Management acknowledges data breech"

An employee violated company policy by using an online service provider to host a document listing some custodian account user names and passwords

Sept 2013

Key lessons learned

Engage all stakeholders

- It is important to have the C-level management team support for promoting awareness and readiness of cyber security risks.
- Cyber security is an enterprise wide initiative and should engage a representative from each participating business unit and step in the value chain.

Know your cyber security landscape

- Always perform an analysis of your cyber security space to understand the actual potential risk, threats and controls.
- Analyse the available options preferably with pilot demonstrations to select the best suited solution(s).

Prioritised approach

- Prioritise the cyber security domain that needs immediate action and plan to approach the needs in a phased manner.
- Focus on the quick wins to earn the support of the involved parties, setting a foundation for the next phases

Not a do-it-yourself or get-it-done space

- Seek expertise on managing and implementing the cyber security governance structure before proceeding with the actual tools and technology.
- Combine expert help with in-house active involvement for a seamless transition to ongoing maintenance, monitoring and pro-active defense.

Cyber security: Do you know how your organisation rates against the following?

You can't secure everything
We will help assess your cyber priorities:
- Enterprise security architecture
- Protect what matters
- Strategy, organisation and governance
- Threat intelligence

It's not if but when
The assessment will cover:
- Continuity and resilience
- Crisis management
- Incident response and forensics
- Monitoring and detection

Fix the basics
The maturity assessment will critically evaluate your security foundation:
- Identify and access management
- Information technology, operations technology and consumer technology
- IT security hygiene and controls alignment to your business processes
- Security intelligence and analytics

Seize the advantage
Our maturity assessment will help you identify digital opportunity with confidence as we will assess key aspects of your cyber strategy:
- Digital trust embedded in the strategy
- Privacy and cyber security legal compliance
- Risk management and risk appetite

Their risk is your risk
Our assessment will review existing cyber risk and provide recommendations to help manage risk in your interconnected business ecosystem.
- Digital channels
- Partner and supplier management
- Robust contracts

People matter
The assessment will assess your cyber maturity in the following key areas:
- Insider threat management
- People and 'moments that matter'
- Security culture and awareness

Why PwC?

Leveraging our deep sector experience in the asset and fund management industry, we understand the complex relationships and interfaces across the value-chain and the underlying potential cyber risk compromise points.

We have performed numerous assessments and evaluations of our clients' cyber security environments and cyber governance models, bringing our global capability and insights to help you assess, design and operationalise a fit-for-purpose cyber security defence and protection plan.

Some of our other cyber security related services consist of the following:
- Cyber risk diagnostic
- Enterprise cyber governance review and development
- Financial crime domain specialists
- Forensic and data driven cyber investigations and threat modelling
- Controlled penetration testing; vulnerability scanning/assessment
- Network security architecture review and design
- Development of comprehensive risk management framework and polices
- Cyber incident response testing and simulation

Key Contacts

Vincent Loy
Partner

T: +65 6236 7498
E: vincent.j.loy@sg.pwc.com

Shong Ye Tan
Partner

T: +65 9820 3623
E: shong.ye.tan@sg.pwc.com

Ervin Jocson
Director

T: +65 8318 1830
E: ervin.jocson@sg.pwc.com

Maggie Leong
Business Development

T: +65 8139 0016
E: maggie.leong@sg.pwc.com

pwc