Cyber Risk and Security for Asset & Wealth Managers (AWM)

12th September 2023

AIMA

wtw

AIMA

Agenda

1. The Cyber Threat Landscape
2. Critical Cyber Controls
3. Building Cyber Resilience
4. Cyber Insurance
    - What is it and how can it help you?
    - Market Conditions
5. Q&A

Presenters

Richard Langdon
Lead Relationship Manager – Asset Management

Dean Chapman
Lead Cyber Risk Consultant (GB)

Huw Dyer
Leader Financial & Professional Lines Cyber & TMT

Cyber Threat Landscape

What are the cyber threats and risks facing the Asset and Wealth Management Sector?

In cyber terms, what exactly are AWMs?

Critical to AWM Businesses

- ✓ Investment & Trading Platforms (technology)
- ✓ Data & Analytics (client, financial, personnel)

Reliance on

- ✓ Availability (of technology / connectivity)
- ✓ Accuracy of Data (integrity and confidentiality)

Business Impacts

- ➢ Disruption to Transactions / Trades
- ➢ Reputational Damage
- ➢ Loss of Clients
- ➢ Financial Costs and Impacts
- ➢ Regulatory Fines or Penalties
- ➢ Any Others?

Why are AWM an attractive target?

What are the cyber threats facing businesses in this sector?

Is your organisation concerned about cyber risk?

AIMA

Critical Cyber Controls

What are the key controls and processes for supporting effective cyber security?

Where and what are your current gaps or exposures?

Most cyber attacks start where and with what?

What key cyber controls should AWMs consider?

Multi-Factor Authentication

- ✓ Additional security 'layer'
- ✓ Hackers love single-factor
- ✓ Widespread deployment

Segregation / Segmentation

- ✓ Reducing 'blast' radius
- ✓ Supports response and recovery
- ✓ Physical and logical segregation

Data Security

- ✓ Encryption at-rest and in-transit
- ✓ Data classification strategy
- ✓ Data breach response plans

Incident Response & Business Continuity

- ✓ Assume breach philosophy
- ✓ Tried and tested > response efficacy
- ✓ Cyber crisis management

Privileged Access Management

- ✓ 'Keys to the Castle'
- ✓ Limit number of privileged users
- ✓ Wider access control management

Backup Strategy

- ✓ Resumption of business operations
- ✓ Multiple formats / locations
- ✓ Restoration testing is a must

Security Testing

- ✓ Internal / External facing systems
- ✓ Structured programme
- ✓ SDLC principles

End of Life / Unsupported

- ✓ Enhanced monitoring
- ✓ Segregation of environments
- ✓ Strategy for decommission

Endpoint Security

- ✓ Endpoint Detection & Response
- ✓ Monitoring
- ✓ Remove administrator privileges

Email Security

- ✓ Email filtering and DLP
- ✓ SPF, DKIM and DMARC a minimum
- ✓ Awareness training is crucial!

Patching & Updates

- ✓ Critical patching process / timeline
- ✓ Formal change management plan

People Security

- ✓ Multi-format training strategy
- ✓ Phishing simulation
- ✓ Assessment of cyber culture

Building Cyber Resilience

How can Asset and Wealth Managers manage cyber threats and risks going forward, are there any other considerations?

- ✓ **Context and Proportionality > Focus on 'Good Enough' Cyber Security**

  'Gold Standard' cyber security is expensive, very expensive – is that what your business needs? Your strategy must be sufficient for and proportionate to your risks and exposures.

- ✓ **Assume Breach Philosophy**

  Allows your business to effectively prepare for cyber security incidents, placing equal time and resources into ensuring your business is able to respond and recover swiftly

- ✓ **Don't Overcomplicate Cyber Risk Management**

  At it's core, cyber risk management boils down to four elements: (1) identify critical assets, (2) gap analysis and assessment, (3) risk treatment, and (4) review, test and manage

- ✓ **Senior Leaders MUST Buy-in**

  Cyber security isn't the preserve of the IT team, intent and commitment to cyber security starts at the top – do your Leaders understand the cyber risks facing your business?

- ✓ **Cyber Crisis Management**

  Whilst technical incident response plans may be in place, do your Leaders understand their role and responsibilities for cyber crisis management? They should...

- ✓ **Cyber Risk Quantification**

  Will provide your stakeholders with financial and monetary contextualisation of your cyber risks and exposures

- ✓ **Can Cyber Insurance Help?**

  Indemnification & Incident Response Support

AIMA

Cyber Insurance

What is it, and how can it help Asset and Wealth Managers respond to and recover from cyber attacks?

Third-party insurance provides coverage for the policyholder's liabilities arising from a cyber incident e.g. damages arising from a data breach.

First-party insurance provides coverage for the policyholder's own expenses arising from a cyber incident e.g. incident response costs arising from a Ransomware attack.

Cyber Insurance – Incident Response Costs

Why are incident response services important for policyholders? E.g. In the event of a data breach.

Coverage (costs for)	Why is it important?	Who is it for?
Incident Response access to 24/7 helpline and experts to triage the event	Under *GDPR*, breaches must be reported to the *ICO* within 72 hours	Policyholders wanting fast access to experts to meet reporting timescales
IT Forensics expertise to help identify, contain the incident & repair the problem	A malicious actor may still be in the network or data may still be leaving the business	Policyholders wanting IT expertise to support their own IT resource
Legal services advice to determine if regulator notification is required	Ambiguity surrounding notification threshold & possible penalties of a given amount	Policyholders wanting legal advice (e.g. *GDPR* notification)
Legal services advice in the drafting & sending notifications to breach victims	Obligation under *GDPR* in certain circumstances and to protect reputation	Policyholders wanting to ensure victims are appropriately notified
Legal services advice around notifying the regulator and help draft notification to the regulator	*GDPR* obligations and ICO advice: "Tell it all, tell it fast and tell the truth"	Policyholders wanting to manage communications with the regulator
Credit Monitoring and ID theft protection services	To protect data breach victims and minimise costs arising out of third party legal proceedings	Policyholders wanting to protect data breach victims from further crime
Call Centres establishing a dedicated call centre to handle enquiries relating to the breach	To manage large volume enquiries and support data breach victims	Policyholders wanting to offer swift communication and support to victims
PR Experts to develop communications strategy and provide breach coaching	To instil confidence, protect brand and avoid a trial by the media	Policyholders that want to protect their brand and reputation

Cyber Insurance

H1 2023 Cyber Market Conditions

Claims & Notifications Frequency & Severity

- Cyber claims frequency increased in the first half of 2023, with third party data breaches and ransomware being the main culprits.
- Ransomware frequency remains high with an increase of almost 20% between 2022 and Q1 2023.
- Cloud exploitation grew by 95% during 2022 according to CrowdStrike's global threat report

Premiums & Retentions Buyers Market

- Pricing in H1 2023 has been more stable than recent quarters, removing exceptionally high and/or low pricing,
- Pricing reductions were achieved with increasing regularity with Reductions of around 10-30% often being available in H1 2023,
- Self-insured retentions were more stable than they have been in the last 12-24 months and insurers have generally been willing to provide alternative lower options /structures.

Policy Coverage War

- The hot topic during H1 2023 has been the war exclusion, following the Lloyd's of London ("Lloyd's") market bulletin of 16 August 2022 which came into effect on 31st March 2023
- WTW's Global Head of Cyber Coverage Andrew Hill has authored a report that addresses the controversy, misconceptions, and more
- The different approaches adopted by insurers to war exclusions has brought into sharper focus **the value of a clear and accurate broking advisory service**. In many cases, any analysis which sets out to demonstrate one war exclusion is 'better' than another exclusion risks overlooking the finer nuances of such a comparison

Market Capacity Buoyant

- H1 2023 has seen **very strong competition from insurers on both primary and excess layers**, with a notable increase in the number of insurers competing for primary positions,
- Market conditions have provided existing cyber insurance buyers with options to purchase increased policy limits.
- Where renewal savings have been generated, clients are increasingly using these savings to **purchase additional capacity** and/or WTW's Restore function via our **CyXS excess facility**.

Key Tips Strategy & Options

- Buyers who see pricing as a key consideration will need to navigate the market with a **well thought out strategy** to ensure the best results are achieved, including factoring-in the amount of capacity they wish to purchase, as this may well impact the overall strategy;
- Given the highly changeable claims trends throughout 2021, 2022 and into 2023**, it feels prudent to expect the unexpected,** suggesting to us that existing cyber insurance buyers should continue to **maximise the opportunities of a more favourable market** to purchase additional limits whilst non-buyers should **review the options available to put cyber insurance in place**

Key Takeaways and Q&A

- Cyber threats and risks continue to evolve and change, and so must our approach to cyber security
- Don’t overcomplicate your cyber risk management strategy – 4-phase approach
- Context and proportionality > a ‘Good Enough’ approach to cyber security
- Assuming breach will help you prepare for the worst > testing your response capability is crucial
- Senior Leaders must be engaged and aware of their roles and responsibilities for cyber crisis management
- The workforce are your greatest asset, but are also the hackers favourite starting point
- Quantifying your cyber risks and exposures will support stakeholders across the entire business
- Cyber insurance isn’t a substitute for effective cyber risk management however, it can be a huge help
- If cyber insurance is being considered, assess your current maturity against the 12 critical controls (page 3)

Richard Langdon
Lead Relationship Manager – Asset Management

Tel: +44 (0) 203 124 8485
Email: Richard.langdon@wtwco.com

Dean Chapman
Lead Cyber Risk Consultant (GB)

Tel: +44 (0) 7872 631006
Email: dean.chapman@wtwco.com

Huw Dyer
Leader Financial & Professional Lines Cyber & TMT

Tel: +44 (0) 7557 590211
Email: huw.dyer@wtwco.com