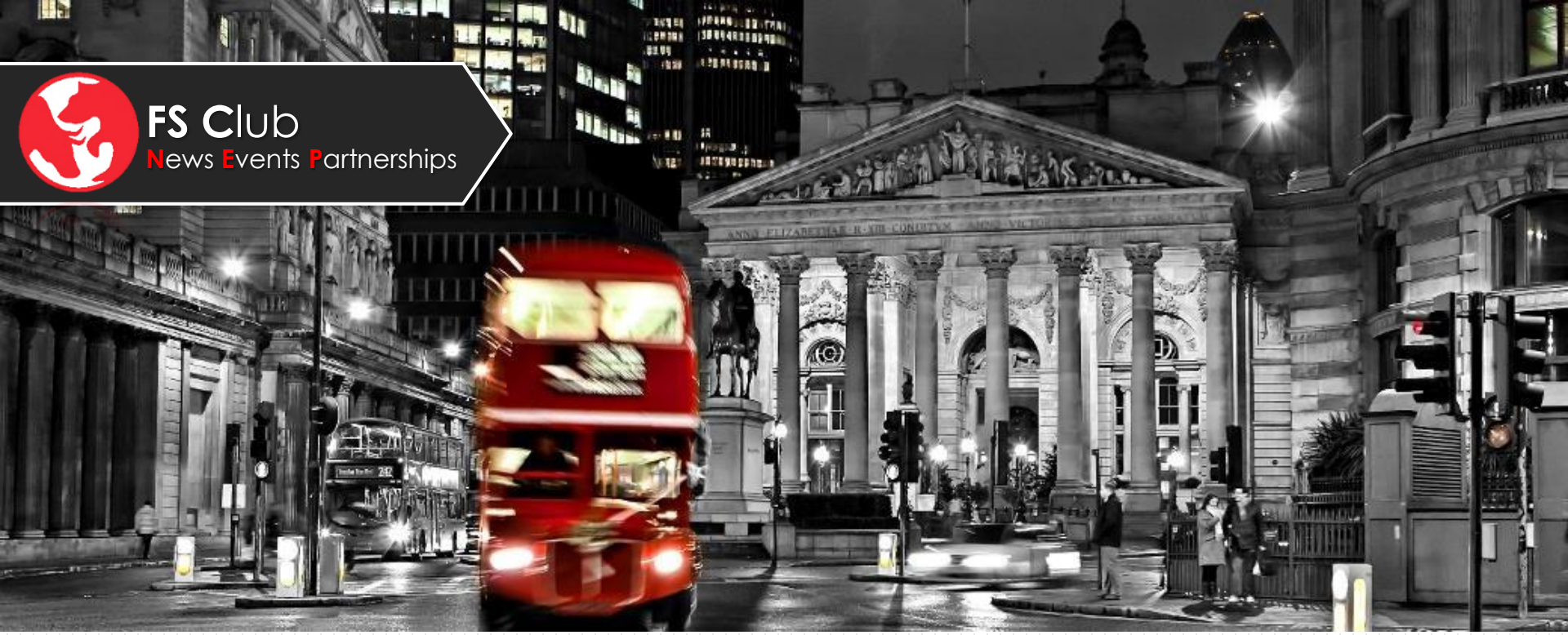


ADDRESSING DATA PRIVACY: MANAGING THE RISK OF FUTURE LIABILITY

With Matthew Negus & Kevin Hall, Alvarez & Marsal, and Hazel Grant, Fieldfisher

Webinar

10am GMT on Thursday, 14 January 2021

A WORD FROM TODAY'S CHAIRMAN

Professor Michael Mainelli

Executive Chairman

Z/Yen Group

FS Club

Platinum Sponsors

Invest Northern Ireland
FINANCE MONTREAL
CDI
GT
Seoul Together we stand
HK FINANCIAL SERVICES DEVELOPMENT COUNCIL
LuxembourgforFinance
CASABLANCA FINANCE CITY
BIFC BUSAN INTERNATIONAL FINANCE CENTER
AIFC
ABU DHABI GLOBAL MARKET
Dubai International Financial Centre

Gold Sponsors

PEERNOVA
Aptitude SOFTWARE
BRIDGEWORKS
FEATURE SPACE
OUTSMART RISK
ARBORETUM
Crown Agents Bank
CERIDIAN

Silver Sponsors

P2 CONSULTING
InfrasoftTech
Bottomline
BCS CONSULTING Expect Excellence
PRAXITY Empowering Business Globally
GPS
The Technium Global SERVICE WITH INTEGRITY

Bronze Sponsors

Profile Software
expleo
CONTACT PARTNERS
alyne
ESTATES AND INFRASTRUCTURE EXCHANGE

Personal Sponsors

Challenge Curve
Currencycloud
worldpay
mastercard
RADIX
ZB
LEI
cuffassociates
Volanté
THE TRANSPARENCY TASKFORCE
CYGNETISE
Catalina Consulting
AMSOM
GIBRALTAR STOCK EXCHANGE

TODAY'S AGENDA

FS Club

- 10:00 – 10:05 Chairman's Introduction
- 10:05 – 10:30 Keynote Addresses
  - Matthew Negus
  - Hazel Grant
  - Kevin Hall
- 10:30 – 10:45 Questions, Answers & Discussion

TODAY'S SPEAKERS

Matthew Negus

Senior Director, Disputes & Investigations

Alvarez & Marsal

Kevin Hall

Senior Director, Cyber Risk Services

Alvarez & Marsal

Hazel Grant

Head of Privacy and Information Law

Fieldfisher

Z/Yen – FS Club

14 January 2021

ALVAREZ & MARSAL
LEADERSHIP. ACTION. RESULTS.

Privacy & Cyber Risk in Corporate Transactions

CONFIDENTIAL – NOT FOR DISTRIBUTION

A&M
LEADERSHIP. ACTION. RESULTS.

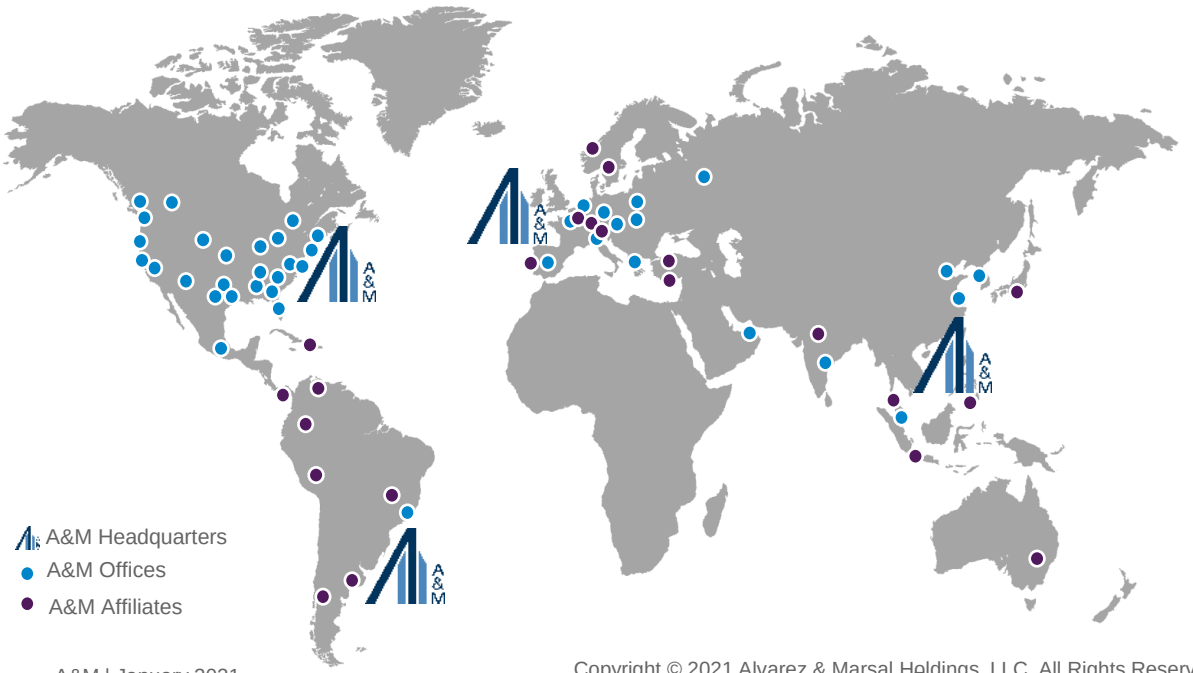
A&M Global Reach

Alvarez & Marsal delivers operational, consulting, investigative and industry expertise to management and investors across the world. We often advise on large-scale global projects, leveraging our experienced network of professionals who reside or work in North America, Latin America, Europe, the Middle East, Africa, Asia, Australia and Russia.

4,500+ PROFESSIONALS

60+ OFFICES

400+ MANAGING DIRECTORS



OUR CLIENTS

- 18 out of 20 of the largest banks in the U.S.
- 95% of the 20 largest European banks
- 80% of the top 20 European law firms
- 300+ mid- and large-cap PE firms
- 68% of all Fortune 100 companies

OUR GLOBAL CAPABILITIES

- Disputes and investigations
- Regulatory and risk advisory
- Transaction advisory and private equity
- Tax advisory
- Turnaround and restructuring
- Performance improvement
- Valuation

ALVAREZ & MARSAL
LEADERSHIP. ACTION. RESULTS.

A QUICK POLL

Has your organisation been involved in any corporate transaction activity (merger, acquisition, divestment) in the last 12 months?

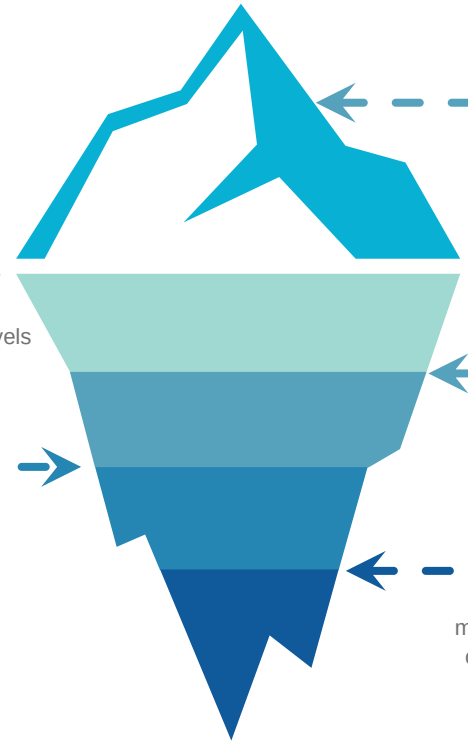
a) Yes

b) No

c) Don't Know

Data Protection in Corporate Transactions

Personal data and the legal and regulatory obligations associated with its use is of particular relevance in the context of corporate transactions including mergers, acquisitions and divestments. As organisations pursue strategic transformation and restructuring, it is critical that adequate time and attention is paid to identifying and measuring risks to personal data within the target organisation. The focus of effort should not be limited to those more 'visible' risk components and due diligence must be 'deep' enough to identify any hidden or less obvious risks to personal data and to realise the full value of data.



Regulatory Filings, Policies, Privacy Notices

Organisations may be tempted to focus on areas perceived to present a 'visible' risk such as notifications with regulatory bodies and privacy notices provided at data collection points

Governance Structure

Determination of whether responsibility for privacy has been designated to individuals within the organisation, resourcing levels are adequate and reporting of activities to senior management

Cross-Border Data Transfers

Identification of cross-border data transfers on both intra and extra company basis relevant to non-obvious business processing activities

Supply Chain & Vendor Relationships

Volume and nature of third-party supplier and vendor relationships, sensitivity of data processing, materiality of services, performance management, contractual safeguards and record-keeping

Data Usage, Legacy Datasets & Retention

Understand extent of personal data usage through data mapping, including identification of data stored on legacy or retired systems and challenges associated with over-retention of data / lack of defined records management

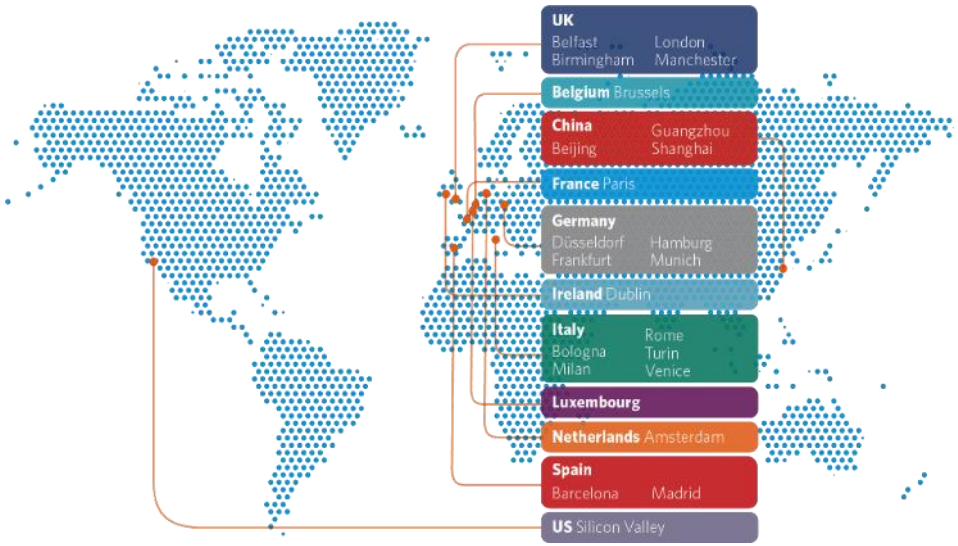
About us

Fieldfisher is a European law firm with market leading practices in many of the world's most dynamic sectors. We are a forward-thinking organisation with a particular focus on technology, finance & financial services and energy & natural resources.

Our growing European network of offices supports an international client base that includes everything from pharmaceutical and medical device companies to energy suppliers, banks and government departments, as well as social media platforms and high street coffee chains. These clients choose to work with us because we deliver commercial, pragmatic and innovative solutions through our exceptional legal expertise and experience – on time and on budget.

We have over 1200 professional advisers spread over 25 locations, all providing highly commercial advice based on an in-depth understanding of our clients' needs. Our clients trust us with work that can have a huge impact on their business or organisation. We have built the firm on people who can be relied on to get it right; they possess exceptional legal knowledge, great market insight and real approachability.

We provide legal advice and services across a range of disciplines. Our pool of lawyers includes many leaders in their field. No matter your particular requirement, we have lawyers with real experience of how your business or organisation works and can provide solutions that are intuitive and relevant.



A SECOND POLL

How would you rate the importance of privacy and cyber risk issues in the context of a corporate transaction?

a) *High*

b) *Moderate-High*

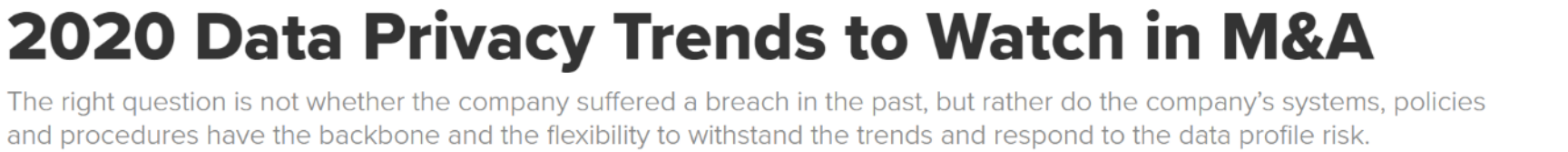
c) *Moderate*

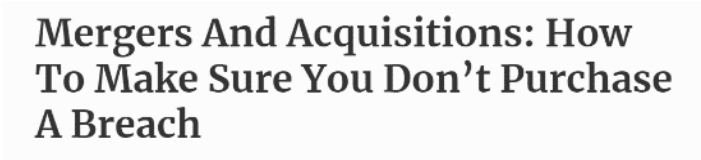
d) *Moderate-Low*

e) *Low or N/A*

Data Protection & Cyber Risk in Corporate Transactions

- **Due diligence is often not adequately assessing risk of regulatory enforcement and litigation due to data compliance**
- **Valuations of data assets and digital strategies need to consider impact of privacy laws including monetisation of user analytics and commercial ability to use and sell data for marketing and consumer profiling**
- **Risk of post-transaction delays or regulatory restrictions where privacy and data compliance is not factored adequately into new corporate structures, business strategy, technology integration and data governance**

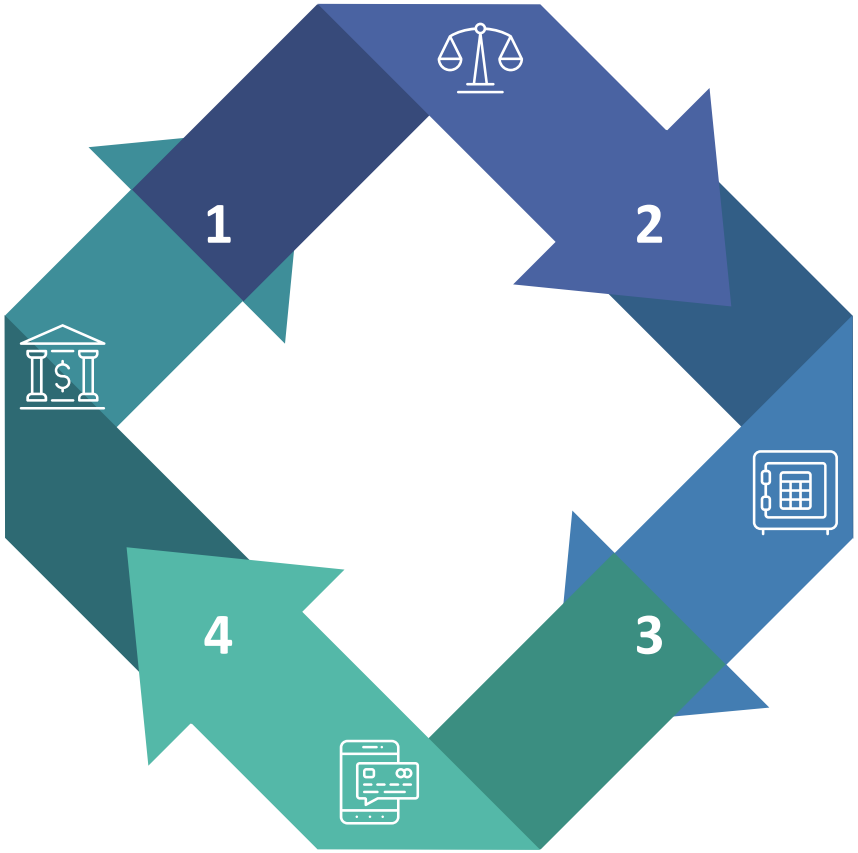




Mergers & Acquisitions – Key Privacy & Cyber Components

Module 1 – Planning

- Acquisition target selection
- Privacy investment/growth potential of target
- Data commercialisation activities (planned/in-progress)



Module 2 – Due Diligence

- Personal data handling lifecycle
- Due diligence risk assessment - individual rights, privacy notices, policies, training, data management, data security, cross-border transfers, vendor risk, privacy impact assessments, data inventories
- Remediation recommendations and roadmap of pre-deal risk items

Module 3 – Deal Closing

- Execution on remediation roadmap
- Privacy governance planning
- Data carve-out (identification)

Module 4 – Post-Deal Integration

- Privacy Office integration
- Operational transition
- Data carve-out (execution)

Divestments – Privacy & Cyber Considerations

4. Post-Separation

Execution of separation activities including data carve-out, updating of group policies, procedures, contracts, notification to regulators, impacted clients and suppliers etc.

3. Deal Closing

Ring-fencing and segregation of shared processes, procedures, third party suppliers, systems and co-mingled datasets (data carve-out) from selling organisation and which require re-papering.

1. Preliminary

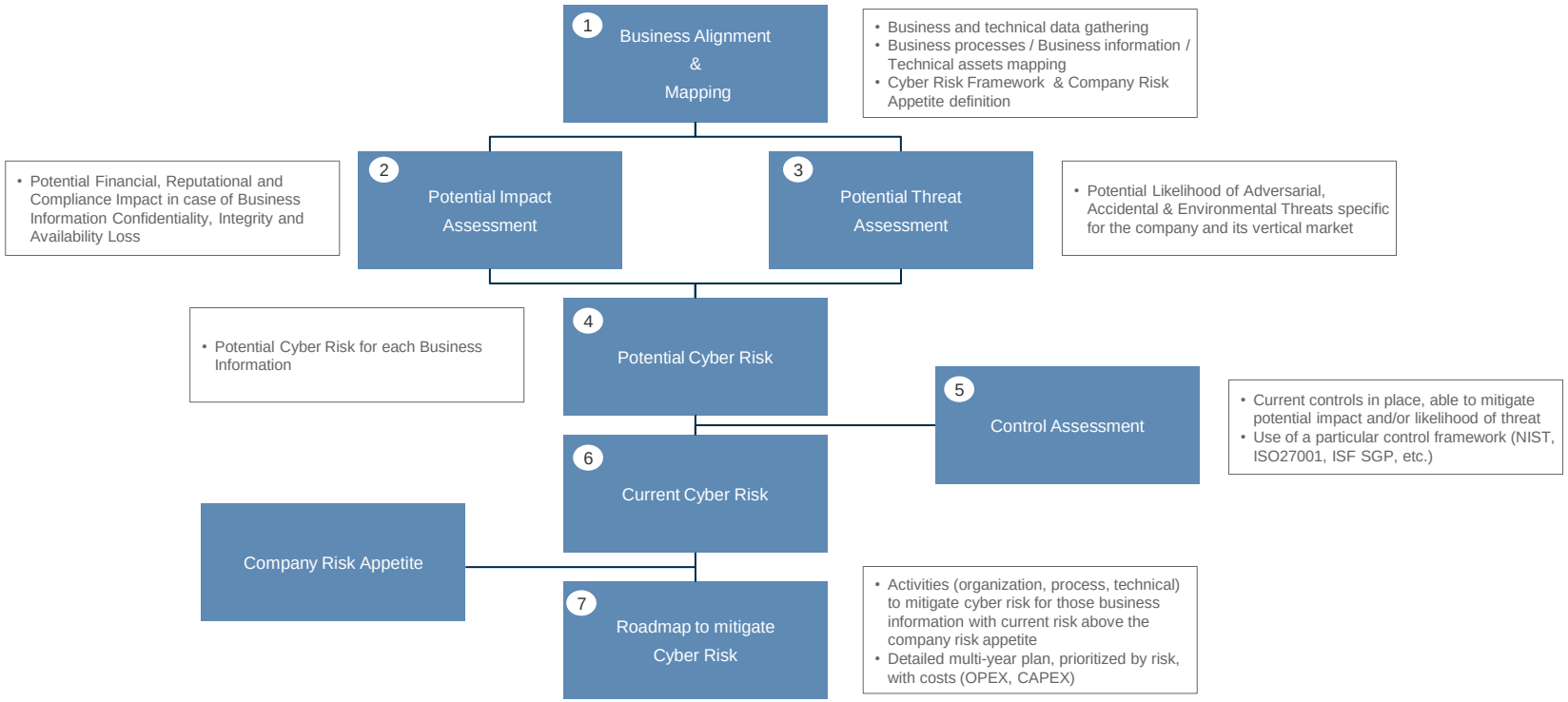
Determination of existing governance, policies, procedures and existing compliance measures to be shared with acquiring organisation in secure data room. Identification of areas likely requiring enhancement pre-transaction.

2. Transition Planning

Identification of shared/joint processes, procedures, third party suppliers, systems and employees requiring separation from selling organisation.

Cyber Risk Evaluation - Methodology

A detailed business risk-based approach to cyber is key for the Board of Directors to prioritize security investment by the reduction of the company risk



Cyber Risk Evaluation – Potential Risk

Obtaining Business Assets and Technical assets classification by potential risk (impact and likelihood of threats)

Business Process/Business Asset/Technical Asset Mapping

Business Process 1	Business Asset 1	Technical Asset 1
Business Process 1	Business Asset X	Technical Asset X
Business Process 2	Business Asset 1	Technical Asset 1

Potential Impact Assessment

Impact	Financial	Reputational	Compliance
High	Loss higher than €3 million	Long term (months) reputational impact, leading to clients relation deterioration, requiring market-wide corrective actions	Inability to meet regulatory or contractual requirements, exposing to severe fines (greater than €250,000)
Medium to High	Loss between €300,000 and €3 million	Medium term (up to one month) reputational impact, leading to clients relation deterioration requiring client-specific corrective actions	Potential exposure to legal actions by individuals
Medium to Low	Loss between €10,000 and €300,000	Short term (up to two weeks) reputational impact, leading to no client relation deterioration, even if clients are informed	Minor fines (between €25,000 and €100,000)
Low	Loss lower than €10,000	No reputational impact perceived internally or externally	No or limited (fines up to €25,000) compliance impact

	Potential impact in case of security incident								
	Confidentiality			Integrity			Availability		
	F	R	C	F	R	C	F	R	C
Business asset 1									
Business asset 2									
Business asset 3									
Business asset 4									

Potential Threat Assessment

Threat Likelihood	Description
High	Event expected to occur more than 10 times a year
Medium-High	Event expected to occur between 1-10 times a year
Medium-Low	Event expected to occur more than once every 10 years
Low	Event expect to occur less than once every 10 years

Threat event type	Threat event	Likelihood value
Authentication attacks	Session hijacking; unauthorised access to legitimate authentication credentials; exploit vulnerable authorization mechanisms	High
Communications attacks	Unauthorised monitoring and/or modification of communications	Medium High
Denial of service	Conduct a denial of service (DoS) attack	Medium High
Information leakage	Exploit insecure disposal of an organisation's information assets	Low
Malware	Introduce malware to information systems	Medium Low
Misconfiguration	Exploit misconfigured information systems; exploit design or configuration issues in an organization's remote access service; exploit poorly-designed network architecture	Medium Low

Cyber Security Due Diligence

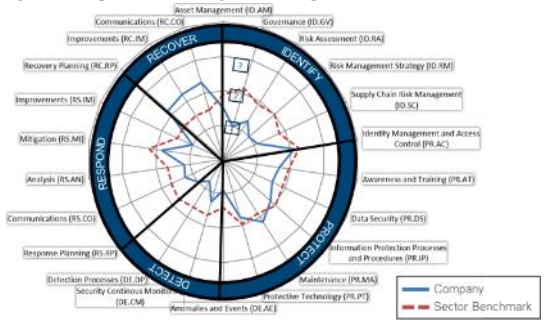
Evaluating the cyber posture of the target is now mandatory as the hidden costs/investments to have an acceptable level of cyber security could be significant

A&M's approach to due diligence is a NIST* based assessment of the company's cyber security posture, against a market benchmark, with prioritised recommendations and a quick win plan (with cost indicators).

Example output: Red flag report findings and recommendations

Area	Maturity	Key Findings	A&M Recommendation	Priority
Organization	◔	▪ Cyber security organization sits inside the IT department, with one dedicated person (CISO) ▪ Cyber security skills appear to be poor ▪ There is no budget specifically allocated to cyber security ▪ Third party cyber security management is well covered	▪ Improve the cyber security governance with clear roles & responsibilities ▪ Improve the cyber security organization by adding two dedicated security engineers ▪ Define a cyber security budget (c.10% of IT)	High
Protection	◑	▪ Basic level of protection i.e., VPN, Firewalls, Microsoft security solutions (Data loss prevention, defender threat protection, anti-virus, data encryption and Multi factor authentication) ▪ There is no anti-DDoS, anti-APT or application level firewall protection ▪ Some customers' information is on unstructured data (MS Excel) and the data does not seem to be clearly mapped	▪ Implement solutions for DDoS and APT ▪ Improve the current anti-malware solution ▪ Implement an Application Level Firewall ▪ Manage unstructured data	Medium
Detection	◔	▪ There is a basic level of monitoring, using a ticketing system to respond to possible attacks, however it relies on the automated firewall and intrusion detection alerts. ▪ There is no Security Operation Centre for continuous security monitoring / triage / assessment, hence it is likely that it is difficult to detect attacks	▪ Implement a Security Operation Centre (external) to monitor and detect security events	High
Response & Recovery	◔	▪ The incident response team uses a response process based on the ticketing system, however, given the poor detection capability, the ability to effectively and efficiently respond to an attack is limited ▪ Recovery from an attack would also be difficult	▪ Implement a Cyber Incident Response Process	High

Example output: Target's maturity score against sector benchmark



Example output: Prioritised cost to fix

Area	Initiative	Priority	Time to Implement	CAPEX	OPEX (yearly)
Organization	Cyber Governance (roles & responsibilities)	High	1 month	xx	xx
	Cyber Team (1-2 additional people)	Medium	1-3 months	xx	xx
	Cyber Security Budget	Medium	N/A	xx	xx
Technical	Manage unstructured data	Medium	3 months	xx	xx
	DDoS solution design and implementation	High	1 month	xx	xx
	APT solution design and implementation (*)	Medium	2 months	xx	xx
	Application Level Firewall design and implementation	High	2 months	xx	xx
Process	Cyber Incident Response Process definition	High	1 month	xx	xx
	SOC design and implementation (MSSP)	High	2 months	xx	xx

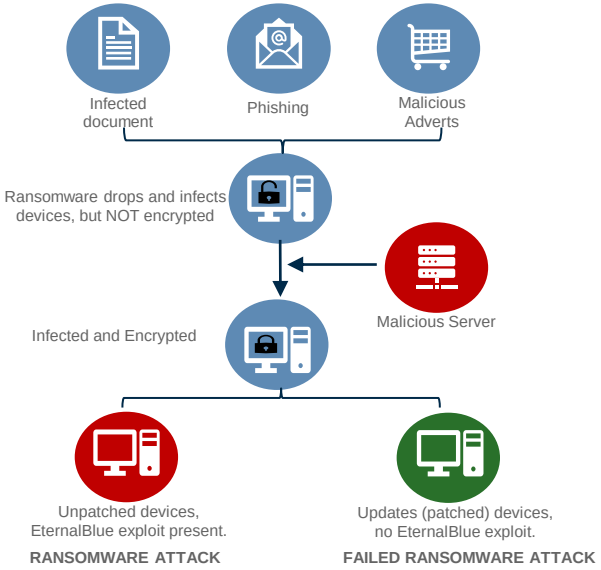
NIST CSF – National Institute of Standards and Technology, Cybersecurity Framework: https://www.nist.gov/cyberframework/framework

Duty of Care

The GDPR tried to embody this important principle*, and it continues to remain the most significant (of the eleven) criteria that regulators are asked to consider when assessing and setting fines following a breach

WANNACRY RANDSOMARE - *HOLDING HEALTHCARE HOSTAGE*

WannaCry (a worn-type self-propagating attack vector) targeted devices running Microsoft Windows OS, encrypting the data and requesting payment in Bitcoin in exchange for their return.



Microsoft had released a patched a month before the exploit occurred. Till date, a number of organisations have not applied the patch and systems continue to remain vulnerable to this exploit.

The Department of Health and Social Care (DHSC) has estimated that WannaCry cost the NHS £92m in direct costs and lost output.

LESSONS LEARNT

Importance of a good cyber security posture including:

- Secure and regular backups
- Proactive cybersecurity software
- Patch management (up to date security patches)
- Isolating Sensitive systems
- Incident response protocols
- User training, awareness and education on 'think secure' measures

Senior Management should ask themselves when thinking about '**reasonable cyber oversight**',

✓ *What will it take to fulfil the directors' duties of care, loyalty and duty to act on an informed basis?*

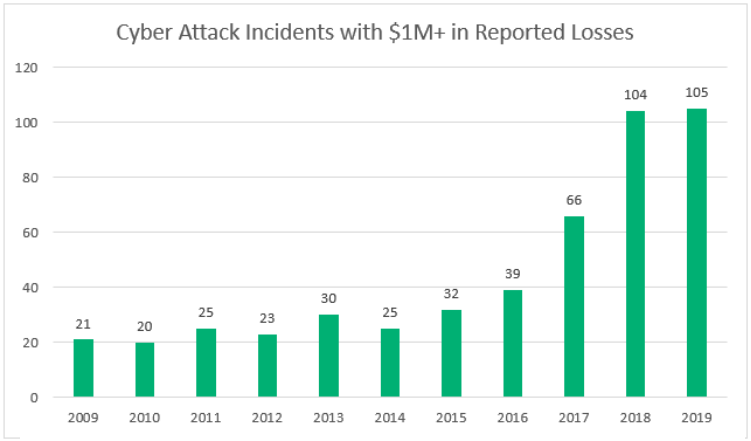
✓ *How does a board avoid creating systematic, sustained or otherwise negligent acts or omissions in how it performs oversight?*

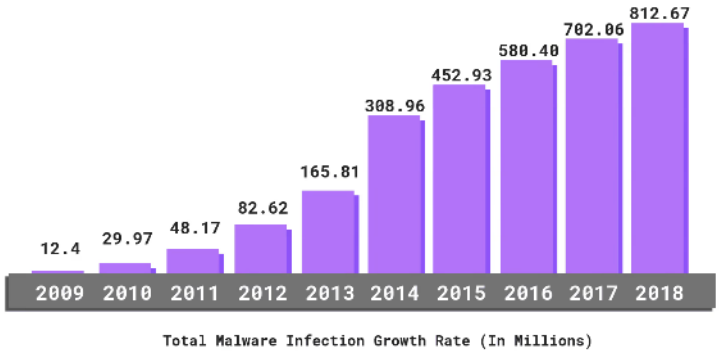
Courts focus on the process used by the board to reach a decision, rather than the decision or outcome itself. In the context of cyber security, the existence of cyber red flags is not, in itself, an indication of director liability or ineffective oversight, but rather paints an emerging picture of the challenges facing the board; **how the board discharges that challenge, or its failure to do so, creates the breach to which personal liability may attach.**

Cyber security attack and spending trend

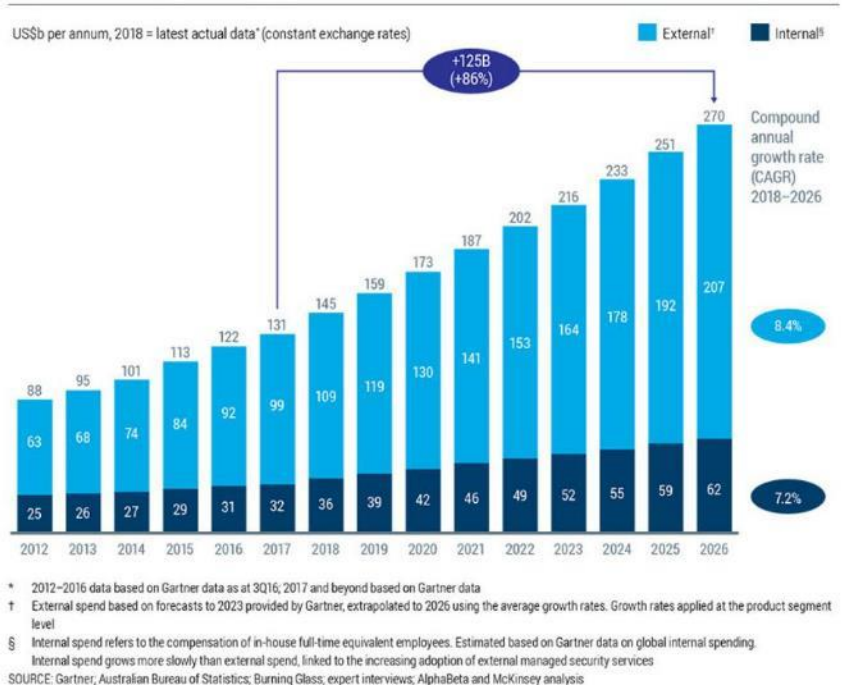
The exponential growth in cybersecurity attacks causing financial losses to businesses has lead to increased cyber spending

Growth in Cyber Attacks





Growth in global cyber security spend



* 2012–2016 data based on Gartner data as at 3Q16; 2017 and beyond based on Gartner data

† External spend based on forecasts to 2023 provided by Gartner, extrapolated to 2026 using the average growth rates. Growth rates applied at the product segment level

§ Internal spend refers to the compensation of in-house full-time equivalent employees. Estimated based on Gartner data on global internal spending. Internal spend grows more slowly than external spend, linked to the increasing adoption of external managed security services

SOURCE: Gartner; Australian Bureau of Statistics; Burning Glass; expert interviews; AlphaBeta and McKinsey analysis

A FINAL POLL

Is Cyber Security and Data Privacy represented in your corporate transaction risk management meetings?

- *Always*
- *Sometimes*
- *Never*
- *Don't know*
- *N/A*

Matthew Negus
Senior Director – Privacy & Data Compliance Services
mnegus@alvarezandmarsal.com
+44(0)7767 102676

Kevin Hall
Senior Director – Cyber Risk Services
khall@alvarezandmarsal.com
+44(0)7765 257451

Hazel Grant, CIPP/E
Partner, Fieldfisher
Hazel.Grant@fieldfisher.com
D:+44 207 861 4217
M:+44 777 572 8838

QUESTIONS AND ANSWERS

FS Club

Platinum Sponsors

Invest Northern Ireland
FINANCE MONTREAL
CDI
GT
Seoul Together we stand
HK FINANCIAL SERVICES DEVELOPMENT COUNCIL
LuxembourgforFinance
CASABLANCA FINANCE CITY
BIFC BUSAN INTERNATIONAL FINANCE CENTER
AIFC
ABU DHABI GLOBAL MARKET
Dubai International Financial Centre

Gold Sponsors

PEERNOVA
Aptitude SOFTWARE
BRIDGEWORKS
FEATURE SPACE
OUTSMART RISK
ARBORETUM
Crown Agents Bank
CERIDIAN

Silver Sponsors

P2 CONSULTING
InfrasoftTech
Bottomline
BCS CONSULTING Expect Excellence
PRAXITY Empowering Business Globally
GPS
The Technium Global SERVICE WITH INTEGRITY

Bronze Sponsors

Profile Software
expleo
CONTACT PARTNERS
alyne
ESTATES AND INFRASTRUCTURE EXCHANGE

Personal Sponsors

Challenge Curve
Currencycloud
worldpay
mastercard
RADIX
ZB
LEI
cuffassociates
Volanté
THE TRANSPARENCY TASKFORCE
CYGNETISE
Catalina Consulting
AMSOM
GIBRALTAR STOCK EXCHANGE

THANK YOU FOR LISTENING

Forthcoming Events

• Friday 15 Jan (12:00)	2021: The Road to Net-Zero Finance
• Monday 18 Jan (10:00)	Patient Capital: The Key To Rebalancing Financial Markets?
• Tuesday 19 Jan (09:00)	Psychology Of Leading A Hybrid Workforce
• Wednesday 20 Jan (09:00)	Financial Centres Of The World 2021: Focus On Dubai
• Thursday 21 Jan (10:00)	An Update On EU Financial Services Legislation & Associated Initiatives
• Friday 22 Jan (12:00)	Owning Your Place In A 21st Century Economy

Visit https://fsclub.zyen.com/events/forthcoming-events/