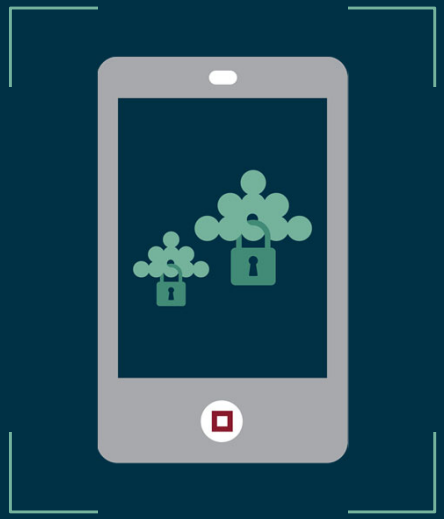
In-House Lawyer Day 2018

Managing risk, protecting reputation

Osborne Clarke



Seminar 1

Data breaches

Ashley Hurst, Charlie Wedin

GDPR | Data breach notification

- Is it really a "data breach"? Avoid that term if possible
- Who is the data controller(s)? A question of fact not contract
- **Article 33 (Regulators):** assess the risk to data subjects – consider preliminary notification
- **Article 34 (Data subjects):** if "high risk" but what is the right thing to do?
- Call / Standard form / letter Whichever the most appropriate
- Insurance

Oh See data incident

Oh See has purchased a licence to a piece of software called iKonect – a smart procurement system to automate customer orders through its supply chain.

On Friday, 16 November at 4pm Oh See becomes aware of a **potential** intrusion into its systems following a data transfer alert from its cyber security software.

Initial forensic investigations indicate that the customer database on iKonect (which is hosted on Amazon Web Services) **may** have been accessed from Oh See's IT system via compromised login credentials of a member of the Oh See IT team.

The iKonect database contains 100,000 customer records, including names, email addresses, home addresses, hashed passwords and purchasing histories.

Indications are that there was an attempt to exfiltrate a large volume of data but it was unsuccessful.

It's Monday morning and Oh See wants to know whether it should notify the ICO and the 100,000 customers potentially affected.

Seminar 2

Business transparency: where risk meets reputation

Dipika Keen, Chris Wrigley, Leanne Coates, Carrie Brassley, Dr Zara Nanu

What is business transparency?

"The mandatory disclosure of previously private business information or data so that it is publicly available."

Targeted action in specific areas

Alternative to quotas / sanctions

Change corporate behaviour by leveraging business stakeholders / risk of reputational damage

Published data can be used as a differentiator (e.g. public procurement)

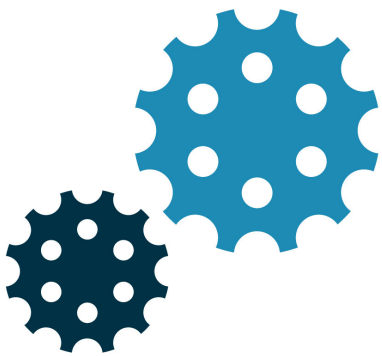
Targeted areas

Ownership

UK corporates

Foreign entities

- holding UK real estate
- bidding for UK public contracts



Supply chains

Modern slavery statements

Payments to suppliers

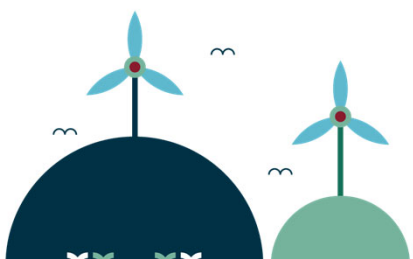
Conflict minerals

Workplace

Gender pay gap

Ethnicity pay

Pay ratios



Environment

Greenhouse gas emissions

Energy usage

What should businesses be doing?

- ✓ **Understand what is on the horizon**

  Long lead times mean you can be prepared

- ✓ **Manage risks triggered by disclosure**

  Reputational, compliance, financial

- ✓ **Exploit opportunities**

  Using data to drive business improvement

  Using disclosures to enhance brand

- ✓ **Take a holistic approach**

  Connect your functions: global compliance programme

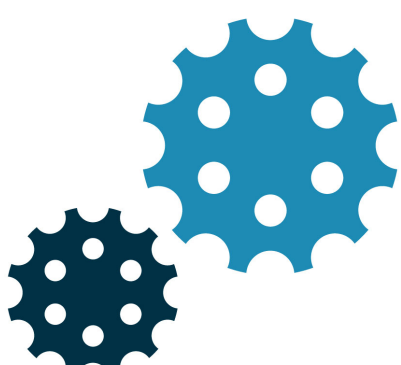
Supply chains

unseen

Understand the benefits

Practical steps

Data collection / trends



Workplace

GAPSQUARE

Gender pay gap 1 year on

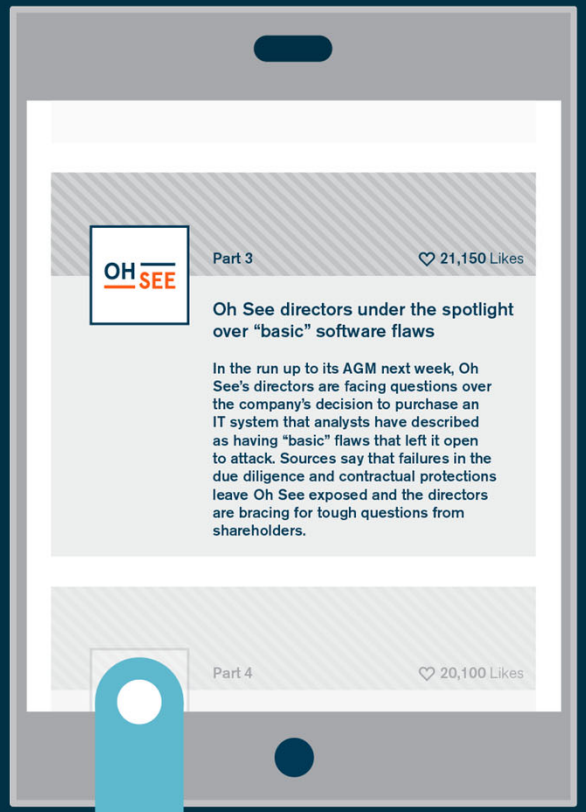
- What have we learned?

Ethnicity pay gap

- What do we know?

Data-led solutions

- What tools are available?



Seminar 3

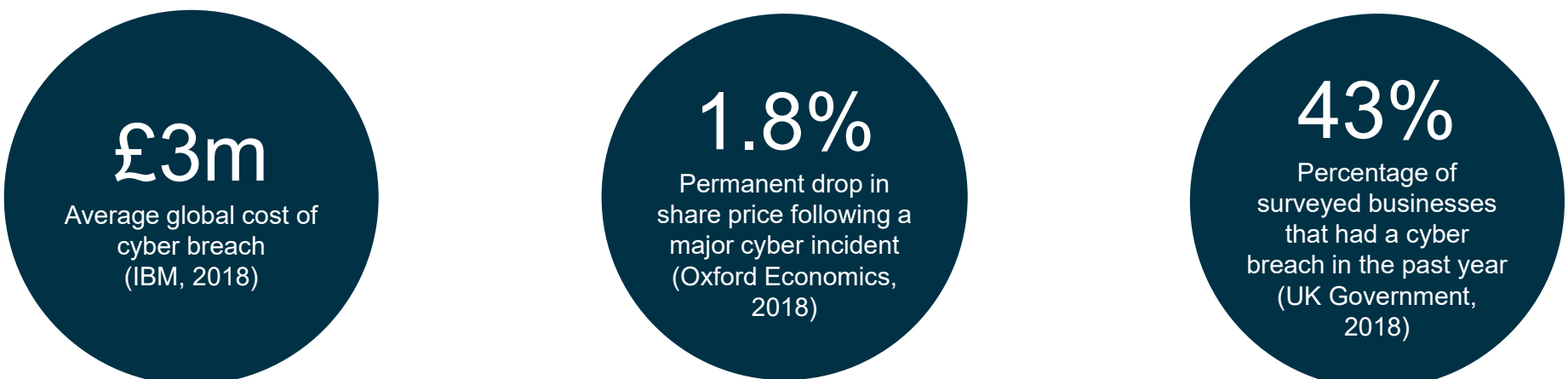
Digital transformation and risk:

Catherine Hammon, Tom Harvey, Katie Vickery, Mark Taylor, Jon Round

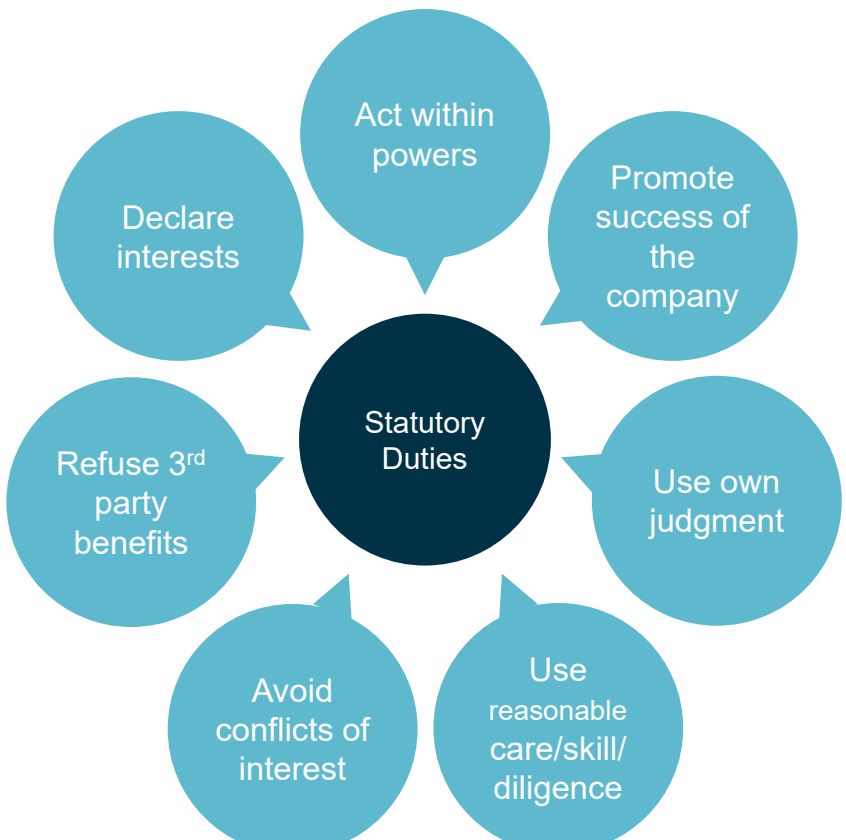
Corporate governance expectations

Tom Harvey

Impact of a cyber breach



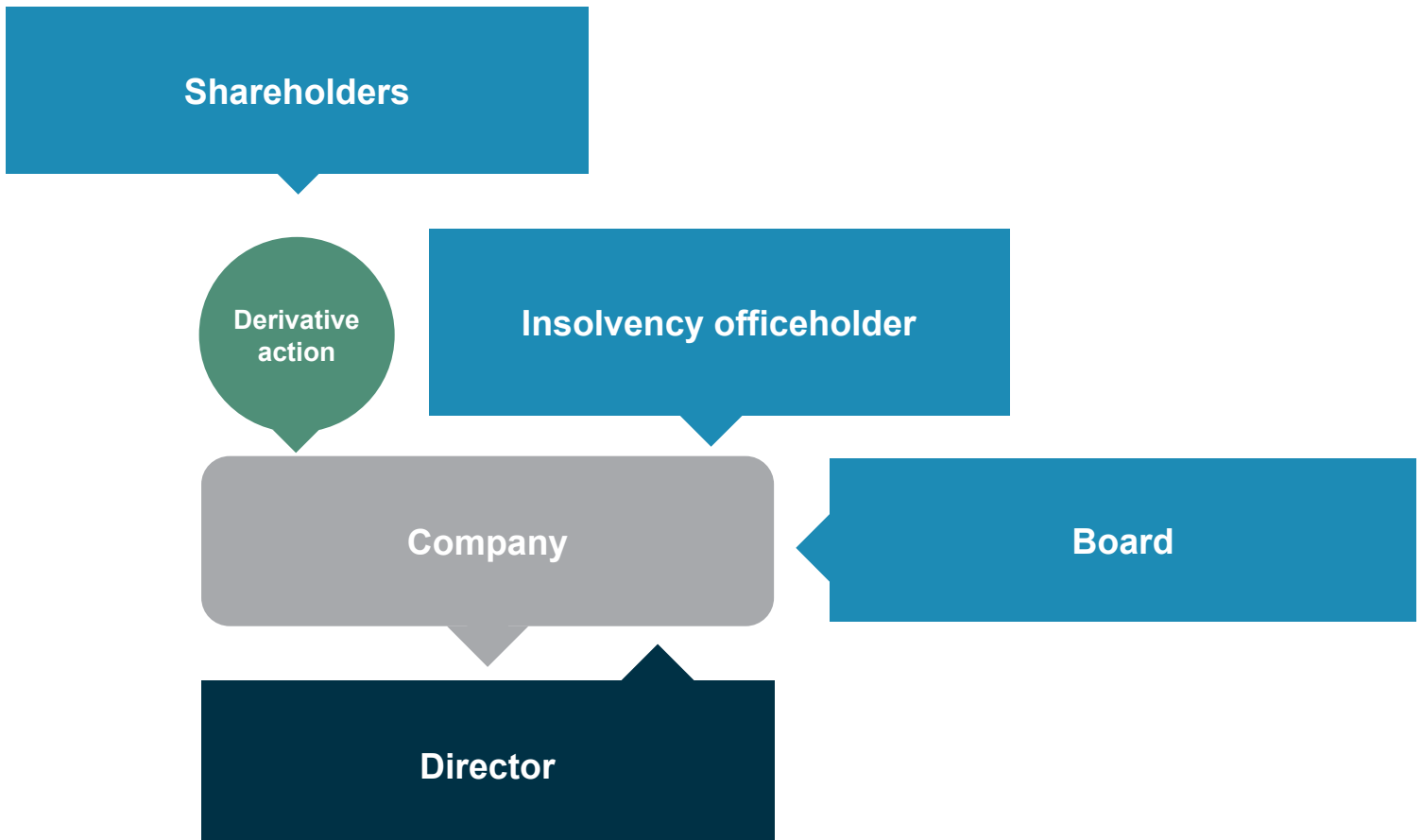
Directors' duties



Protect creditors in insolvency

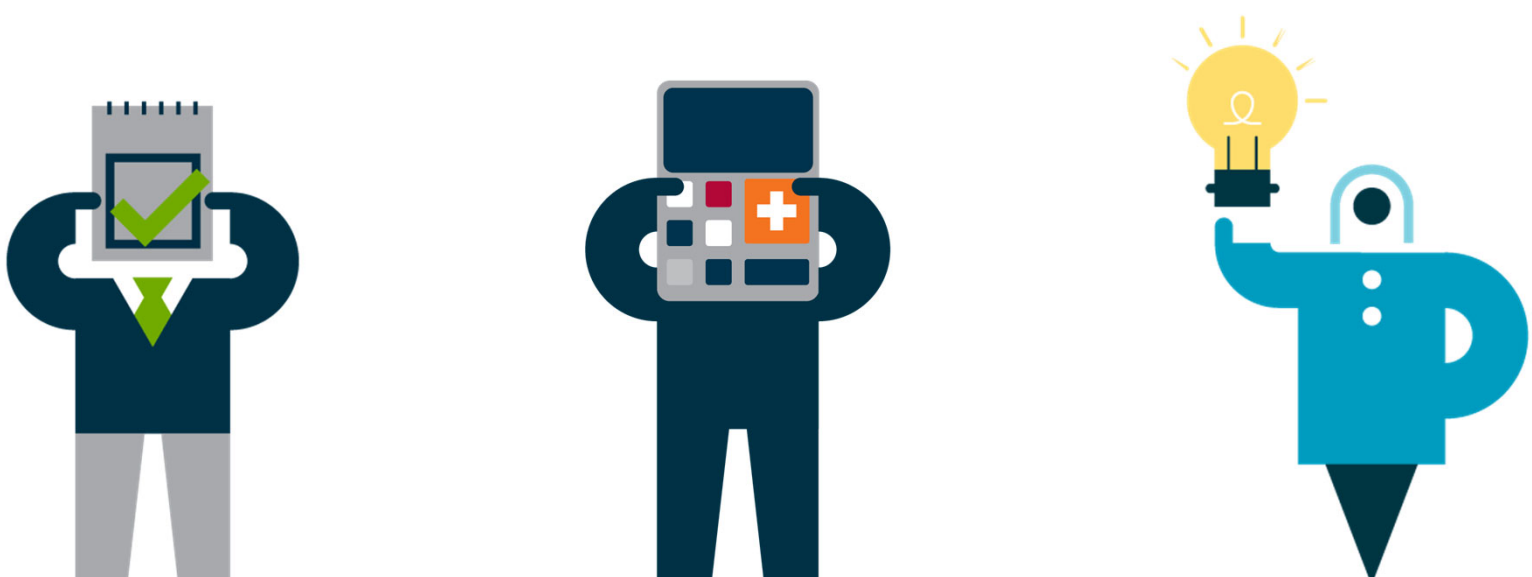
Confidentiality

Enforcing the duties

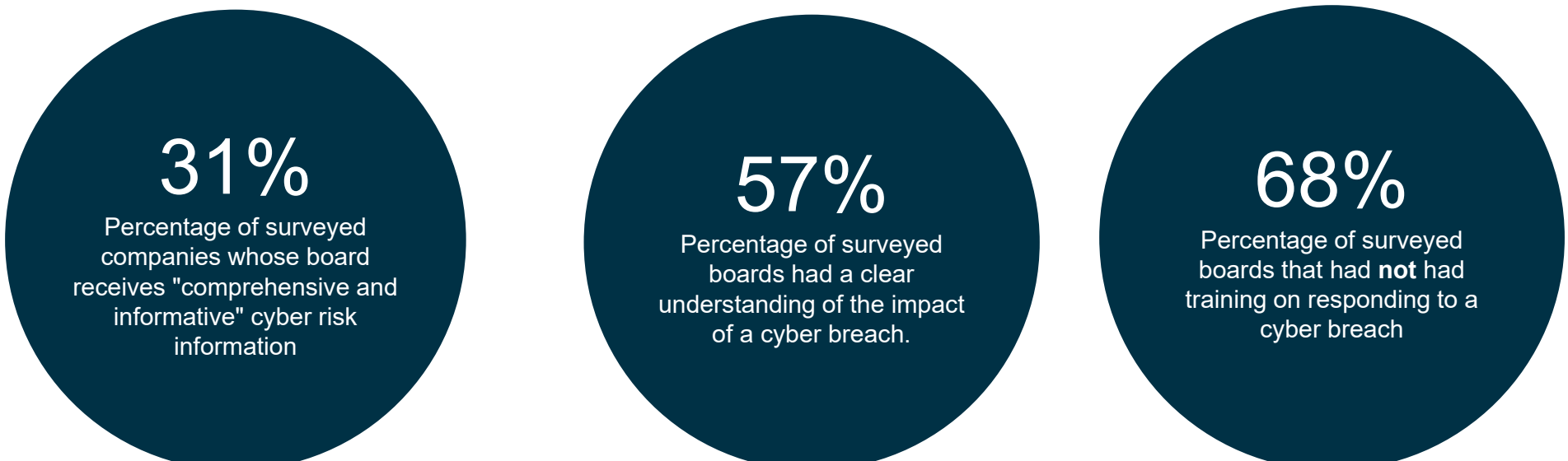


Exercising reasonable care skill and diligence

"A director must exercise reasonable care, skill and diligence"



FTSE 350 Cyber Governance Health Check Report 2017



The hardening attitude of institutional investors

“Investors need to discuss these issues at the highest level with board directors to raise awareness and get the board involved. [Cybersecurity] is a key operational and financial risk, not something just left for the IT department to deal with. This issue will only intensify in the future, so investors need to start the conversation with companies today to better understand their exposure.”

- Legal and General Investment Management (2017)

"Consistent dialogue on this topic will indicate to companies that cyber security is a priority issue for investors and, as such, should be incorporated into corporate reporting… Through private dialogue, investors may also want to probe the reasons for poor public disclosure and explore how related challenges may be overcome."

- PRI (2018)

UK Corporate Governance Code guidance

The board should establish procedures to manage risk, oversee the internal control framework, and determine the nature and extent of the principal risks the company is willing to take in order to achieve its long-term strategic objectives.

The board should carry out a robust assessment of the company's emerging and principal risks. The board should confirm in the annual report that it has completed this assessment, including a description of its principal risks, what procedures are in place to identify emerging risks, and an explanation of how these are being managed or mitigated.

Making sure the board gets it right

- Exercise effective oversight of cyber security issues
- Review and evaluate management approaches to cyber security
- Ensure alignment of the cyber security programme to business risk profile
- Ensure effective allocation of resources and expertise to cyber issues
- Ensure public disclosures are an accurate reflection of cyber risks and incidents

Sources of help

PRI report "Stepping up governance on cyber security" (2018)
investors' viewpoint on cybersecurity

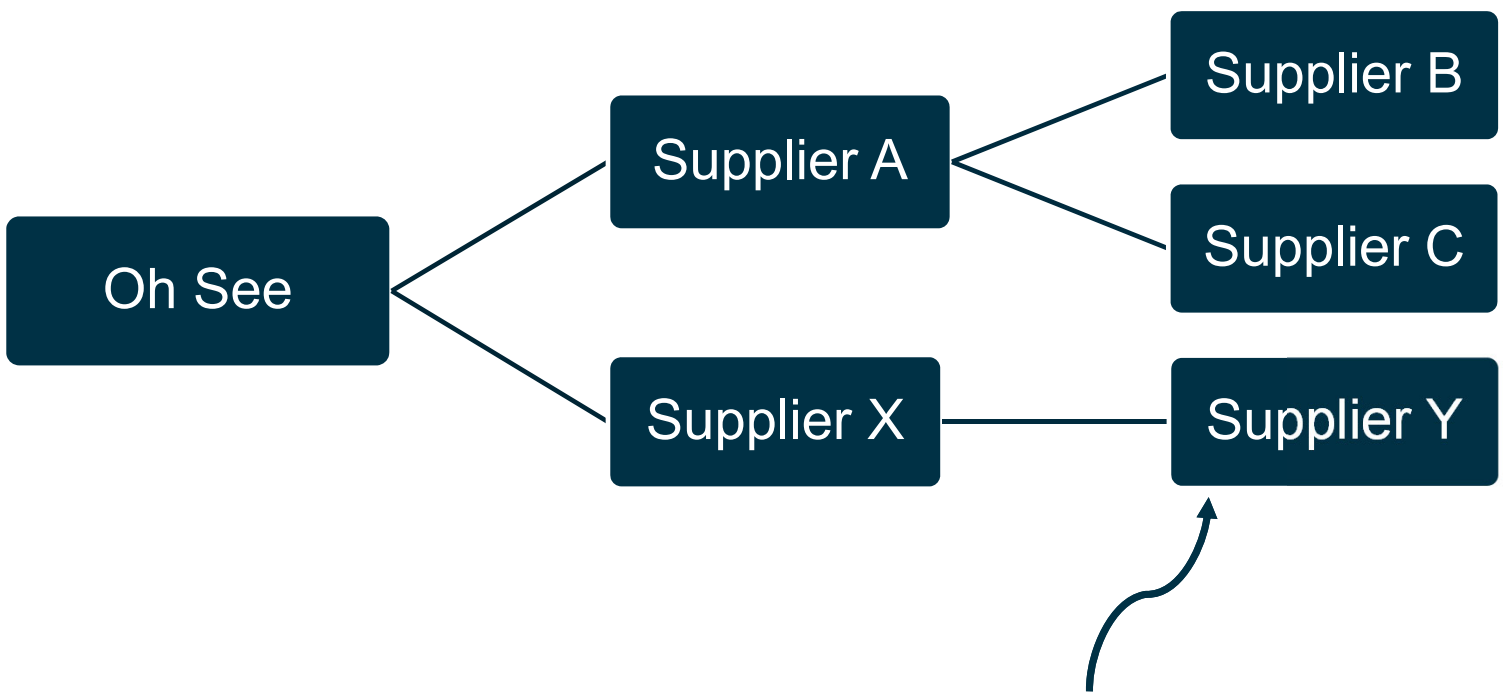
FRC Lab Report on Risk and Viability Reporting (2017)
Examples of best practice in corporate reporting

FRC Guidance on Risk Management (2014)
Detailed guidance supporting principles on risk management set out in the UK Corporate Governance Code

Cybersecurity in the supply chain

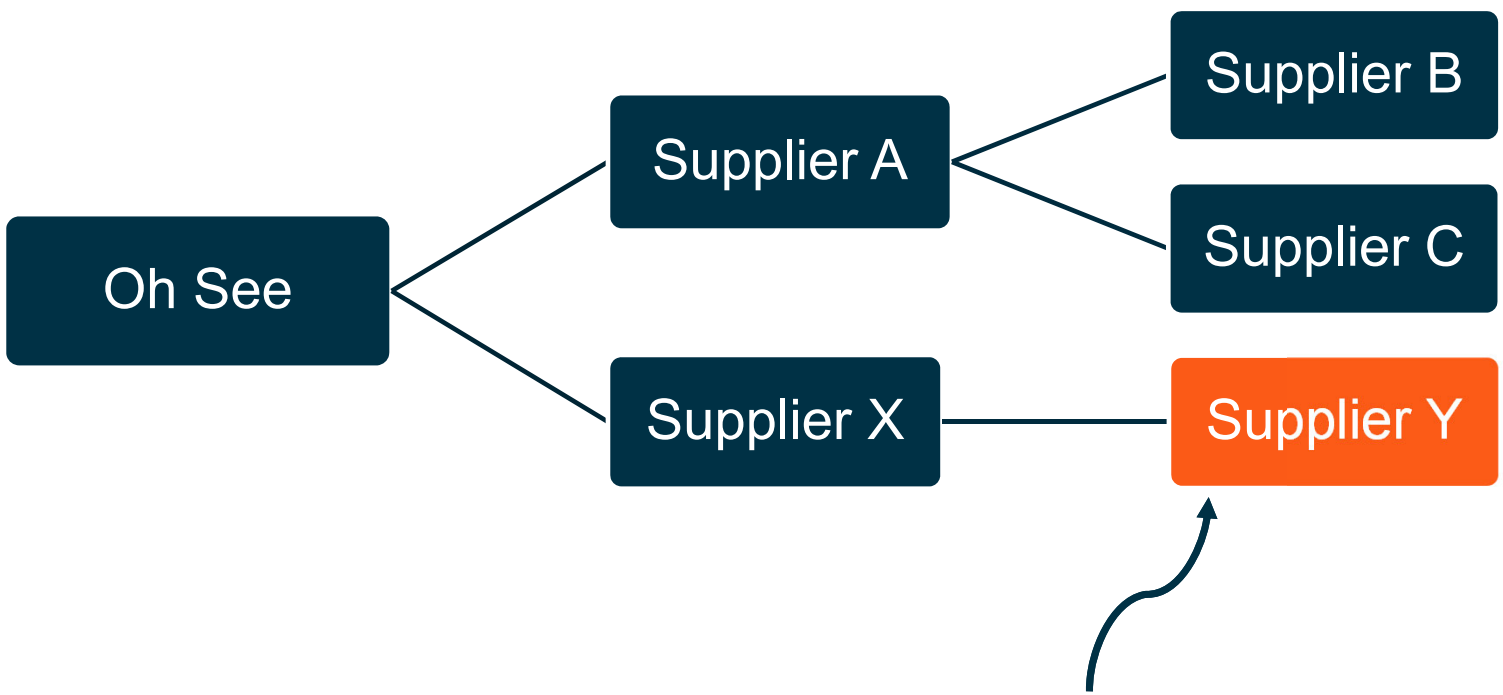
Jon Round

The Threat



Various vulnerable points in supply chain

The Threat



Cyber strength of an organisation that relies on a chain only as strong as the weakest member of the chain

The threat

Does Oh See have established procedures for managing cyber risks in its supply chain?

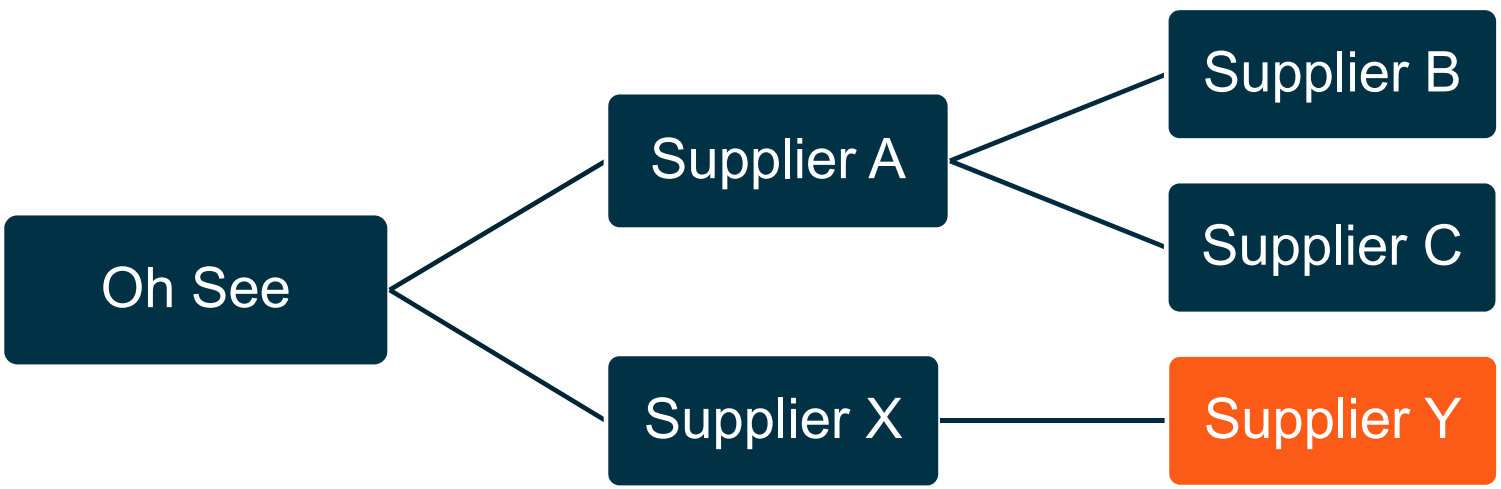
Has it followed these procedures?

Records of organisations with which Oh See shares sensitive information?

Does Oh See know:

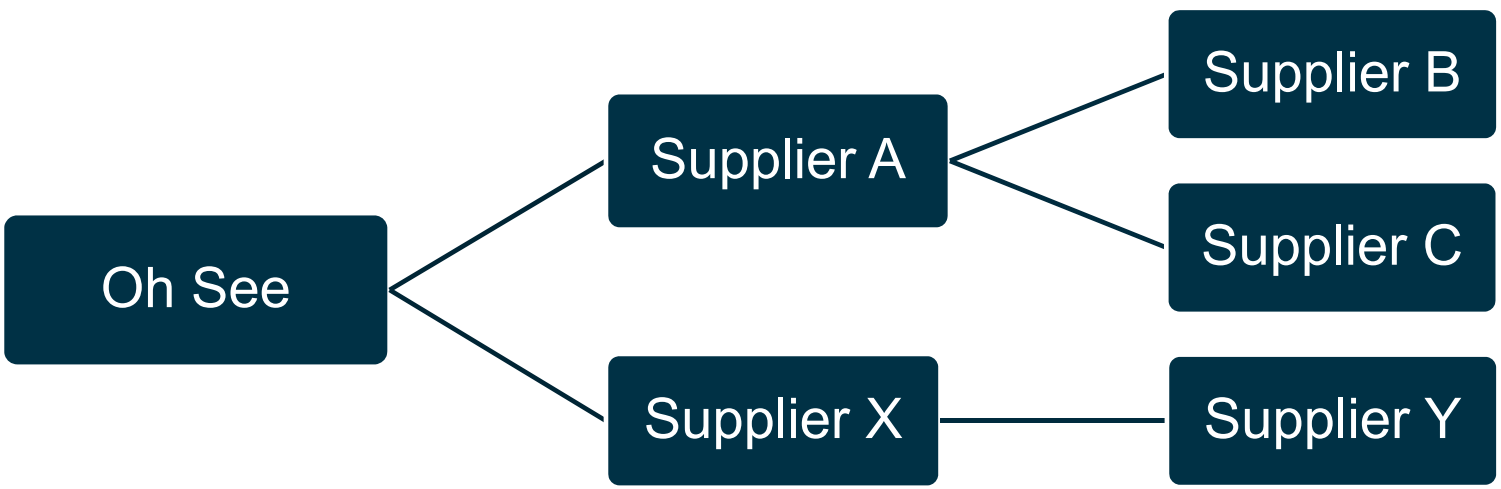
- whether its suppliers share that data?
- what contractual protections are in place?

Improve defence



Identify key cyber exposure in your supply chain + carry out DD

Improve defence



Understand the flow through from suppliers to products / services

Improve defence

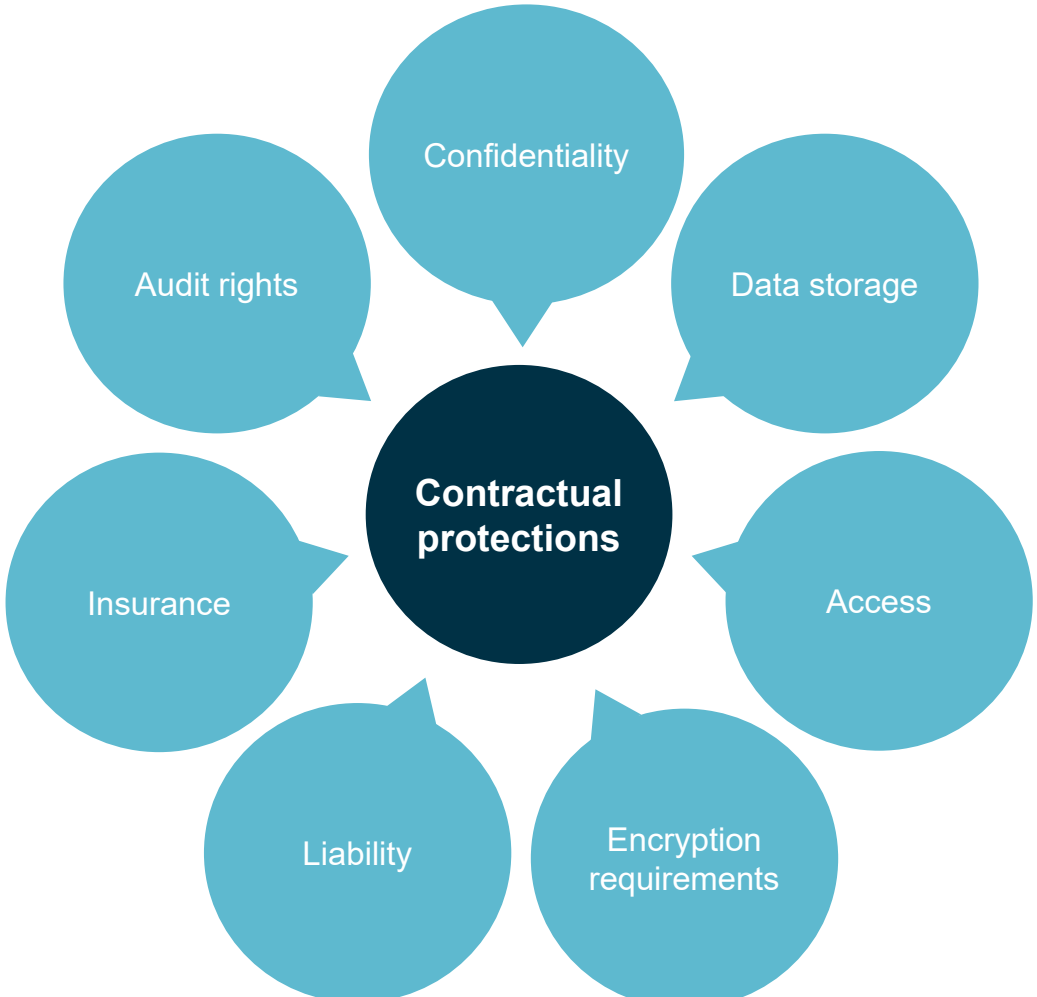
Identify your cyber requirements

Review cyber policies of suppliers

Minimum security policy for suppliers to observe?

Improve defence

Ensure key protections in supply chain contracts



Improve detection

Use contractual rights to regularly audit suppliers' cyber security

Require contractual reporting, with clarity on:

- Notification trigger
- What must be reported
- Contact points
- Timeframes

Improve response

✓ Draft cyber breach response plan

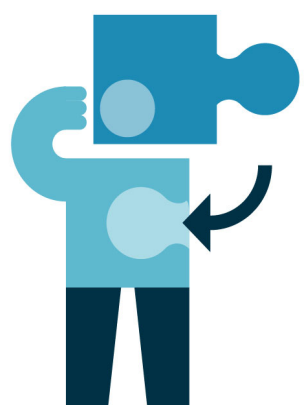
Reflect need for assistance in supply chain contracts

✓ Consider specific cyber insurance

For your organisation and its suppliers

✓ Have a record of contractual breach notifications

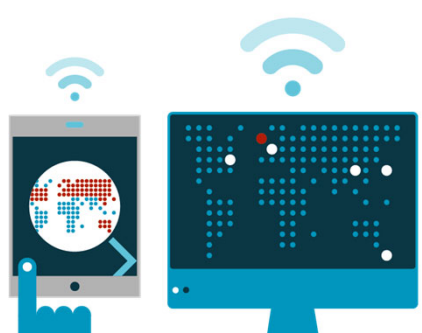
Including which systems / services they relate to



Cybersecurity and consumer law

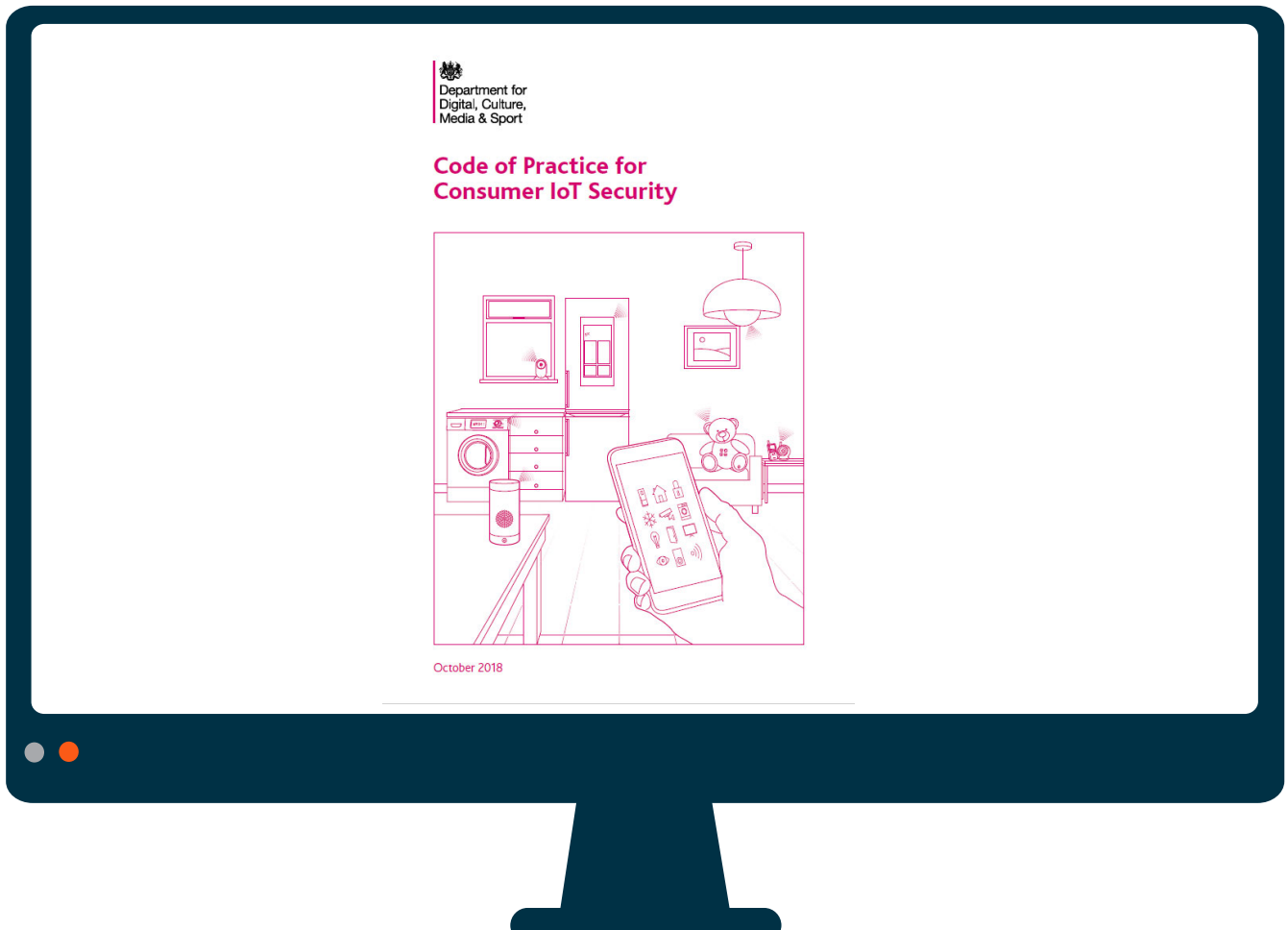
Katie Vickery

"….the UK household ownership of smart devices could rise from approximately ten, to fifteen devices per household by 2020"



Connected consumer products

Code of practice



13 Guidelines

Device Manufacturer	IOT Service Provider	Mobile Application Developers	Retailers
12 Guidelines apply	11 Guidelines apply	8 Guidelines apply	1 Guideline applies

Guideline 1

No default passwords

Passwords are unique and not resettable to any universal factory default.

Guideline 2

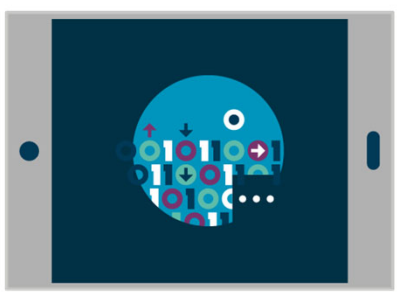
Implement a vulnerability disclosure policy

Companies that provide internet-connected devices and services shall provide a public point of contact to whom issues can be reported as part of its policy.

Guideline 3

Keep software updated

Updates shall be secure, timely and should not impact on the functioning of the device.



Consumers should understand the need for each update and also when updates for the device will stop.

Guidelines 4-13

4 Securely store credentials and security-sensitive data

5 Communicate securely

6 Minimise exposed attack surfaces

7 Ensure software integrity

8 Ensure that personal data is protected

9 Make systems resilient to outages

10 Monitor system telemetry data

11 Make it easy for consumers to delete personal data

12 Make installation and maintenance of devices easy

13 Validate input data

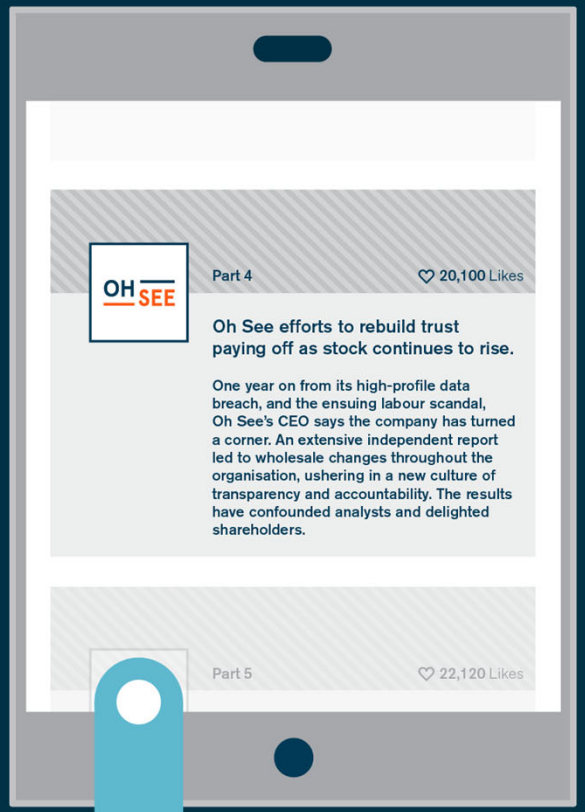
The legal implications

Consumer IOT device placed "on the market"

Cyber attack

Failure to meet "essential requirements"
(i) health and safety
(ii) the protection of property?

Defective product?



Breakout session: option A

Short-term pain, long-term gain

Tom Ellis, Katie Vickery, Chris Wrigley

What are we going to cover?

Starting point: following through on Investigation Report Recommendations

Getting Practical: who is responsible and what is happening?

Is technology the answer?

Turning crisis and compliance shortfalls into a positive force

Following through on Investigation Report Recommendations

Following through on Investigation Report Recommendations

Discussion question

Have you used a particular approach, technique, or strategy, which has helped you ensure your business follows recommendations?

Getting Practical:
Who is responsible,
What is happening
And is technology the answer?

Getting Practical: who is responsible, what is happening and is technology the answer?

Discussion questions

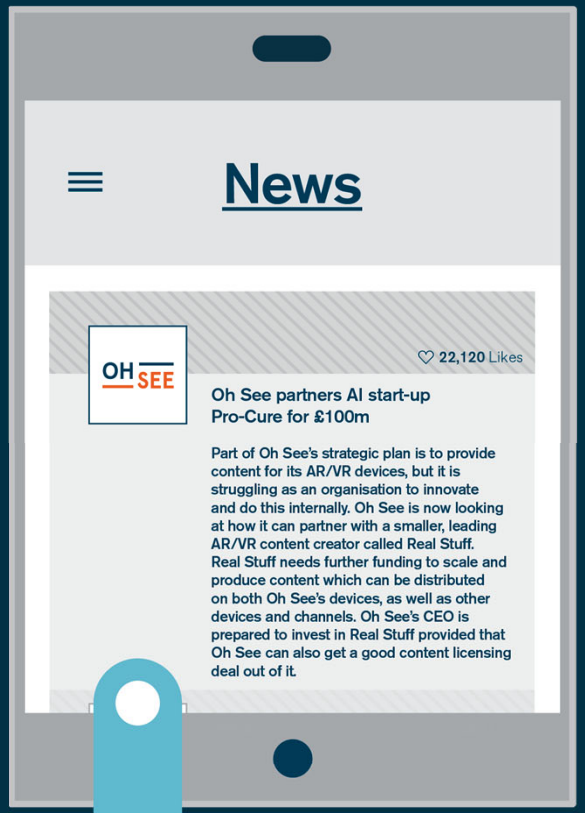
Do you use specific technology to monitor or actively control compliance systems?

Turning crisis and compliance shortfalls into a positive force

Turning crisis and compliance shortfalls into a positive force

Discussion questions

What techniques (large or small) has (or could) your business use to drive its compliance culture?

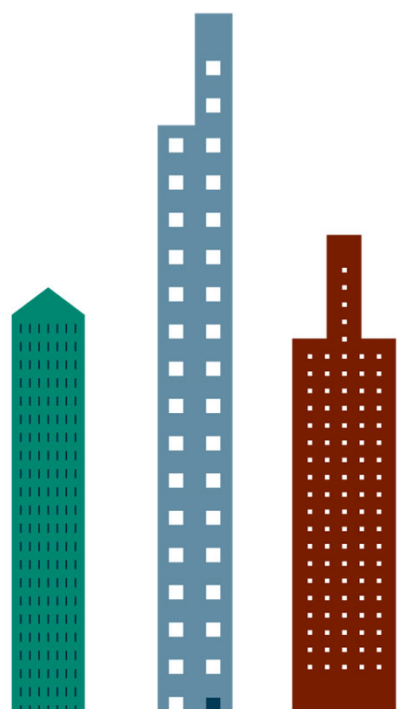


Breakout session: option B

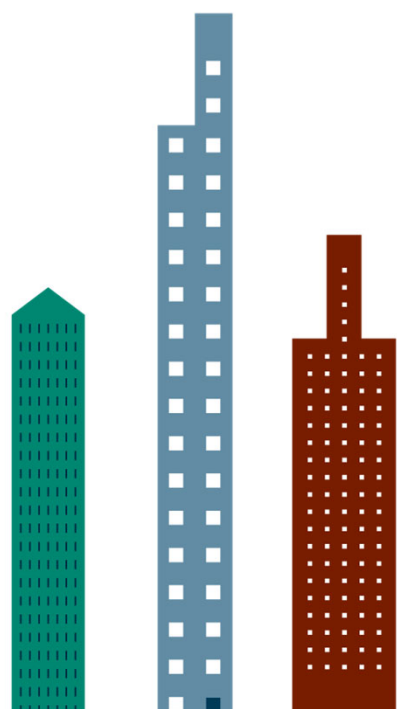
Corporate venturing

Mathias Loertscher

What is corporate venture capital (CVC)?



CVC corporate structure



Context for the investment

Key documents:

- Subscription Agreement
- Shareholders' Agreement
- Articles of Association
- Commercial agreement?

Other parties:

- Investee company
- Founders/Management
- Angel investors/Friends & Family
- Institutional venture capital funds
- Other CVCs?

Key terms and legal considerations

- Share rights
- Board governance
- Consent matters
- Information rights
- Commercial arrangements
- Exits

Subscribing for shares

Key terms of the Subscription Agreement

Initial investment for shares

Additional investment option or obligation?

Warranties

Share rights

CVC class of shares: normally a class of **preferred shares**

Share Right	Preferred Shares
Voting	• Rank alongside other shares and voting pro rata to number of shares held? • Enhanced voting rights for CVCs?
Income (dividends)	• Rank alongside other shares and dividends paid pro rata to number of shares held? • Preferential dividends – fixed dividends (% of investment) or participating dividends ahead of ordinary shares; cumulative if not paid?

Share rights (cont'd)

Share Right	Preferred Shares

Capital (return of capital or sale)	• Rank ahead of ordinary shares (and earlier preferred shares?) on return of capital or sale
	• "Participating" or "non-participating":
	  • **Participating**: entitled to both amount paid for shares (or a multiple of it) and to participate in the balance of proceeds available pro rata with the ordinary shares;
	  • **Non-participating:** entitled to the ***higher of*** amount paid for shares (or a multiple of it) and amount which they would receive if shares were converted into ordinary shares and participated pro rata.

Share rights (cont'd)

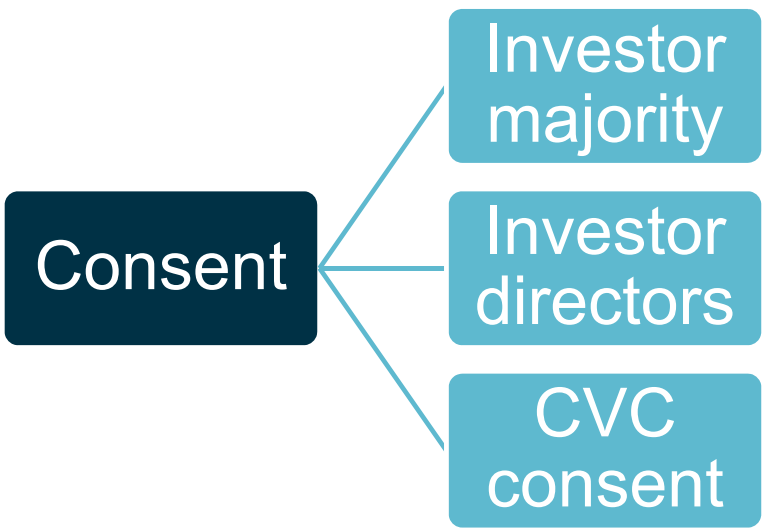
Share Right	Preferred Shares
Pre-emption rights	• Right to participate in future share allotments and share transfers • Should investors have priority over other shareholders?
Drag Along	• Prescribed majority of shareholders to have right to compel other shareholders to sell their shares as part of a sale • Does the investor need to be part of dragging majority? • If not, in what circumstances can the investor be dragged (and to whom)?
Co-Sale Rights	• Right to sell a proportionate number of shares if a Founder (or sometimes any other shareholder) sells shares
Tag Along	• If there is a share transfer which would trigger a change of control, the other shareholders are entitled to sell their shares at the same time and on the same terms

Board governance

What is the **board composition** and what rights (if any) does the CVC have to appoint a director?

Consent matters

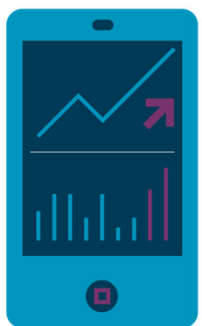
Certain important company actions may require CVC consent



CVC Specific Issues

Positive Undertakings

Information rights



Financial information

Trading updates

Exit offers and discussions

Commercial arrangements

Timing:	• Co-ordinating signing of the commercial deal with closing the funding round can be challenging
Condition to completion:	• Desire to complete commercial arrangements will depend on significance/ value of commercial arrangement vs financial investment for both sides
Alternatives:	• If fully negotiated agreement is not possible before signing, consider alternatives (MOU or similar)
Connection to shareholder rights:	• CVC investor rights may be tied to benefits under commercial arrangement being realised by the company
Benefit or burden:	• If commercial arrangement is too "extractive" or focuses the company's development too much on the CVC, CVC's investment may be less attractive

Exits

Path to control

ROFR / matching rights

Drag along rights

Competitors