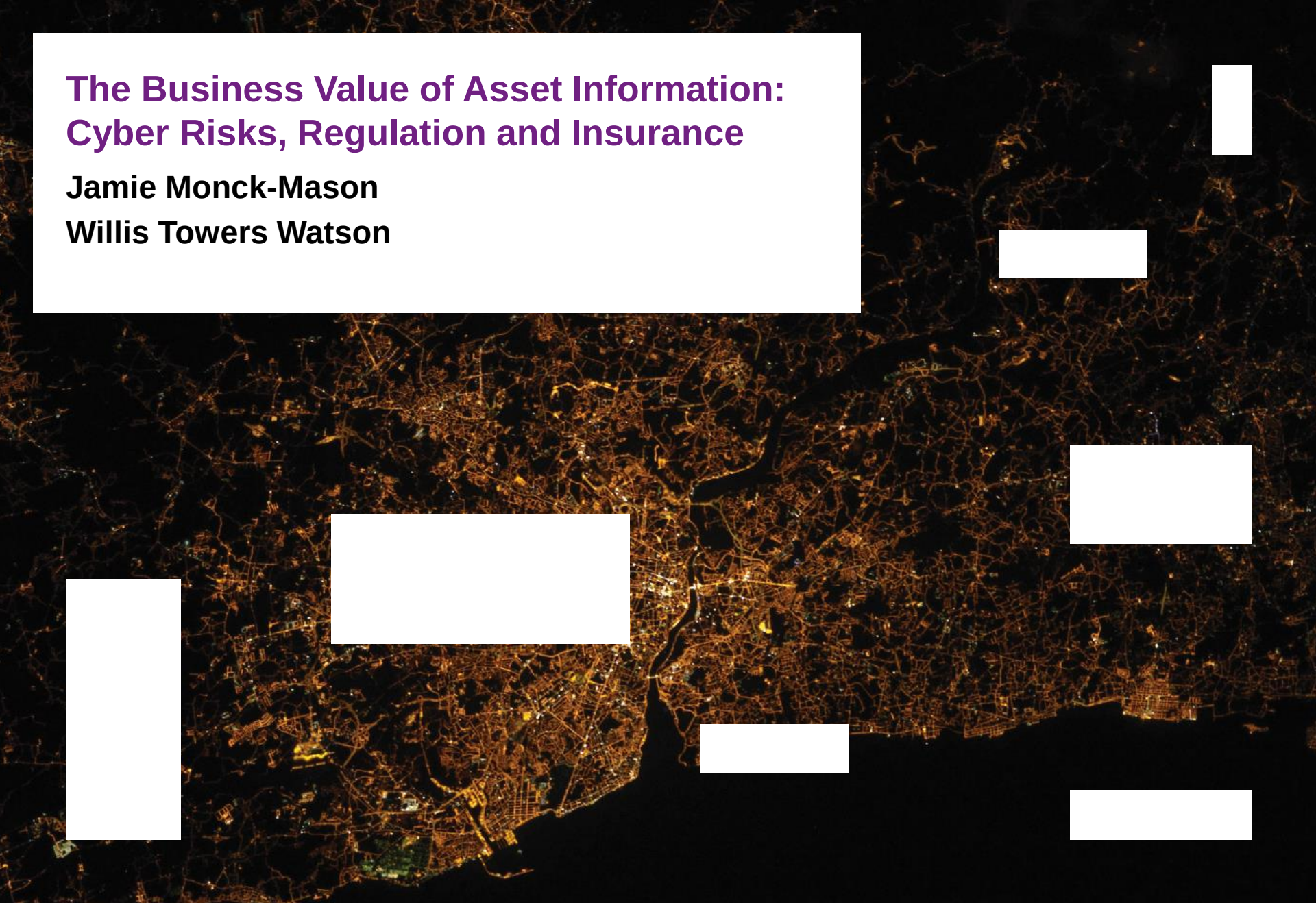
The Business Value of Asset Information: Cyber Risks, Regulation and Insurance

Jamie Monck-Mason

Willis Towers Watson



Willis Towers Watson

The Cyber Risks Landscape: Some Emerging Trends I

Indiscriminatory Attacks

- **A still frequently asked question: “Why should anyone want to attack my business?”**
- **Ransomware attacks (Wannacry, (Not)Petya) are the commonest attacks giving rise to cyber insurance claims.**
- **Not targeted. Volume is the key, exploiting widely used (usually venerable) software. Low ransoms.**
- **Not just the cost of dealing with the extortion threat itself: business interruption loss and reputational damage.**

The Cyber Risks Landscape: Some Emerging Trends II

System Failure and the People Problem

- **Cyber crime and state-sponsored attacks understandably steal the limelight. 18% of cyber incidents are caused by external threats.**
- **Don't forget system failure (human error and technical failure).**
- **Some examples from the aviation world: Southwest, Delta and BA.**
- **Don't just focus on cyber defences: consider the cyber risk culture within the organisation. Employee negligence and malfeasance play a role in 66% of cyber incidents. Promote staff training and instil a cyber-savvy culture from the top. Insurers are increasingly mindful.**

The Regulatory Landscape I

General Data Protection Regulation (GDPR) 25 May 2018

- **Mandatory notification of data breaches to regulator within 72 hours and to data subjects without undue delay.**
- **Requirement to appoint a DPO in certain circumstances.**
- **Data subject rights re portability, erasure and objections to automated profiling. Action within 1 month. Compensation for financial and non-financial damage (distress) and class actions.**
- **Extra-territorial scope.**
- **Requirement to "demonstrate compliance" with GDPR principles.**
- **Fines of up to 4% of annual global turnover or EUR20m whichever is greater.**
- **23% companies say they'll be non-compliant, or only partly compliant, by 25 May**

The Regulatory Landscape II

Network and Information Systems Directive (NISD) 9 May 2018

- Operators of "essential services" (OESs) and digital service providers (DSPs) must maintain "appropriate and proportionate" cyber security measures to prevent disruption to those services. Again, this is extra-territorial in scope.

- "Essential services" are those which are "essential for the maintenance of critical societal and/or economic activities" and which depend on network and information systems: providers of water, electricity, oil, gas, petroleum, NHS trusts, airports, air traffic control, large airlines, harbour authorities, terminal operators, large freight carriers, road authorities, rail companies and Network Rail, and digital infrastructure (top level domain name registries, domain name service providers and internet exchange point operators).

- DSPs include online search engines, cloud computing services and online marketplaces.

- OESs and DSPs must notify serious cyber incidents to competent authorities (eg Dept for Business, Energy and Industrial Strategy, DfT, Dept of Health, DDCMS) or Computer Security Incident Response Teams (CSIRTs) within 72 hours.

- Fines of up to 4% of annual global turnover or EUR20m whichever is greater.

The Insurance Response I

Historically

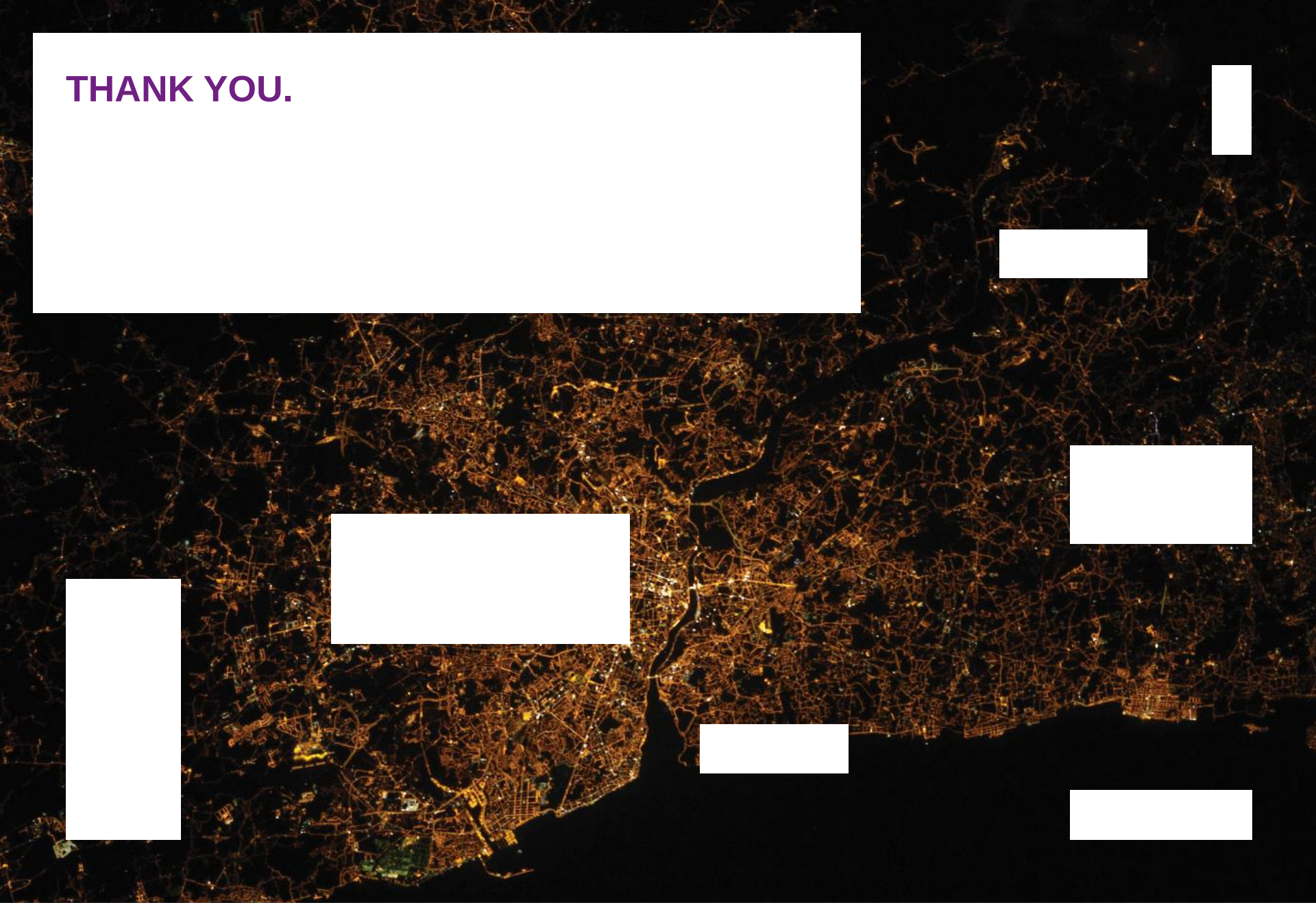
- Cyber insurance evolved to meet the costs of responding to (and notifying) data breaches (and associated regulatory, PCI exposures and third party privacy liabilities) particularly in the US.
- Fit for purpose re data breaches, but plagued by inconsistency of coverage and US-biased wordings issues.
- Less mature as insurance for non-physical business interruption losses: issues over high time retentions, restrictive cover (cyber attacks against insured's own system) and the costs and delays in settling claims.
- Issues over insurers' readiness to take policy points over failure to update/patch regularly.
- Sometimes issues over capacity.

The Insurance Response II

Looking Ahead

- **Greater appreciation of the differences in legal frameworks outside the US (reflecting expanded pool of cyber expertise in London in particular).**
- **More consistency in insurers' offerings.**
- **Improved cover for business interruption: lower time retentions, optional extensions of cover to system failures and outages sustained by critical third party systems and progress in settling claims promptly (and innovation around these issues).**
- **Recognition by leading cyber insurers that they cannot afford to take policy points over IT updates without damaging their credibility (although the Equifax breach has seen a revival of insurers' interest in patching).**
- **Ever increasing capacity.**
- **Further appetite for innovation.**

THANK YOU.



Willis Towers Watson