A ‘VIEW FROM THE TOP’ OF UPCOMING GOVERNMENT LEGISLATION/ REGULATIONS RELATING TO CYBER SECURITY

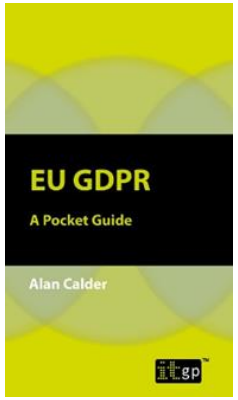
Presented by:

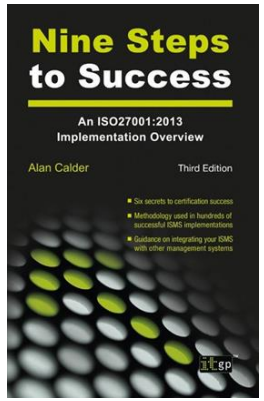
- Alan Calder, Founder and CEO
- IT Governance
- 6 June 2019

Introduction

Alan Calder

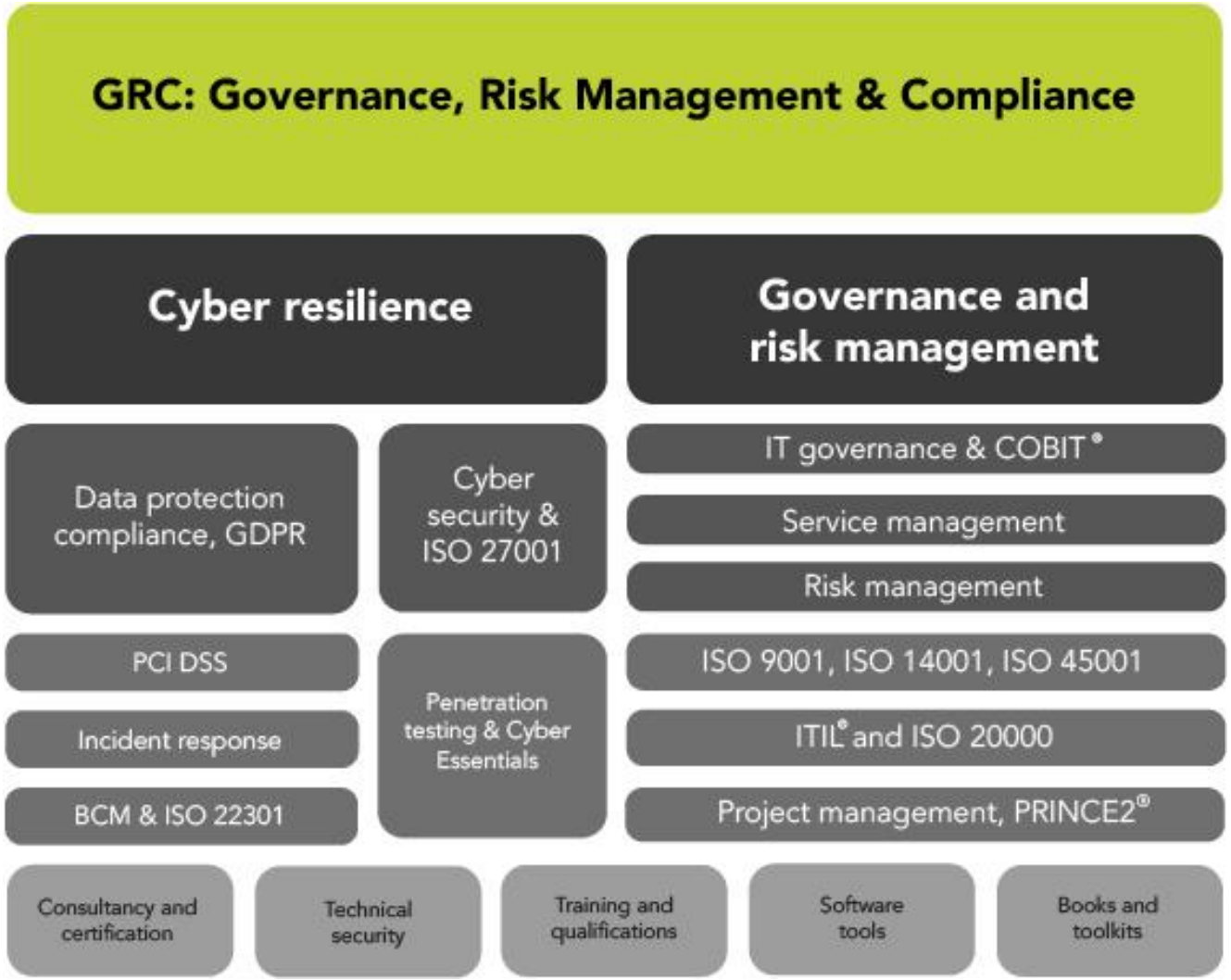
- Founder and executive chairman of IT Governance
- IT Governance is the leading global provider of IT governance, risk management and compliance solutions
- Author of IT Governance: An International Guide to Data Security and ISO27001/ISO27002 and EU GDPR Pocket Guide



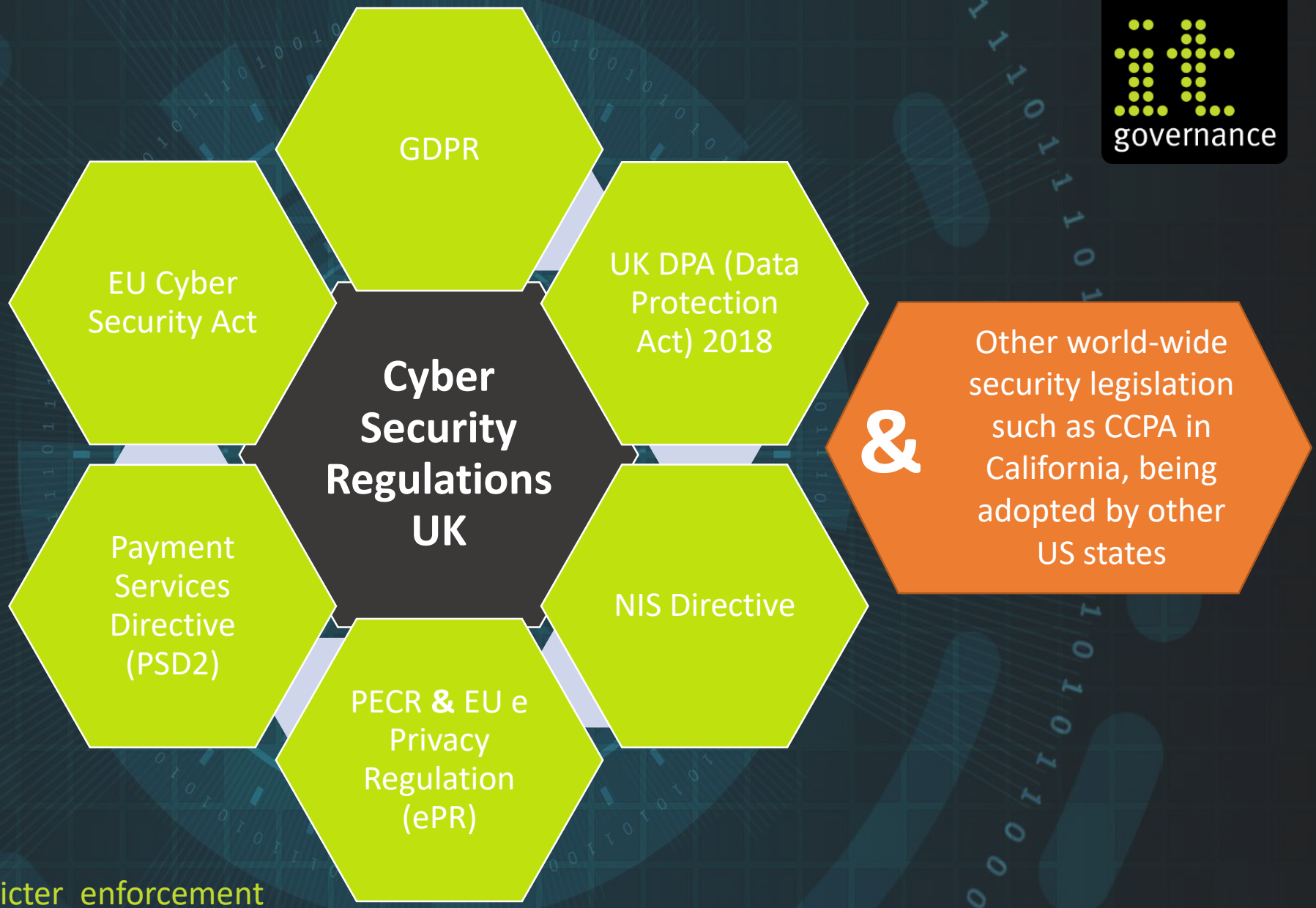


Protect • Comply • Thrive

IT Governance: GRC one-stop-shop



A ‘VIEW FROM THE TOP’ OF UPCOMING GOVERNMENT LEGISLATION AND REGULATIONS RELATED TO CYBER SECURITY



'Light touch' giving way to stricter enforcement

The GDPR and the DPA 2018

- The EU GDPR (Regulation 2016/679) has been in place in all EU member states since 25 May 2018.
- In the UK, the new DPA was enacted in May 2018 to make GDPR part of UK law, irrespective of Brexit and to supplement the EU GDPR.
    - Data subjects have the right to lodge a complaint with the supervisory authority (the ICO) if they consider that the processing of their personal data infringes the Regulation.
    - Data breaches have to be reported to the ICO.
    - Higher penalties than the DPA 1998. The GDPR and DPA are backed by fines of up to €20 million (about £17 million) or 4% of annual global turnover – whichever is greater.
    - Allows for class actions
- Key areas of risk: data subject complaints, reportable breaches.
- Enforcement action in the offing.

The NIS Directive

- The **EU's NIS Directive (Directive on security of network and information systems)** is the first piece of EU-wide cyber security legislation. It was enacted in the UK Law as the *The Network and Information Systems Regulations 2018* on 10 May 2018.

- The NIS Directive:
  - Aims to **achieve a high common level of network and information system security** across the EU's critical infrastructure.
  - Applies to **OES (operators of essential services)** in the UK's energy, transport, health, water and digital infrastructure sectors
  - Applies to **DSPs (digital service providers**), which are divided into three groups: online search engines, online marketplaces and Cloud computing services.

- Member states are required to set their own rules on financial penalties and take the measures to ensure that they are implemented.

- In the UK, non-compliant organisations may be fined up to £17 million.

The PECR & ePR

- The PECR (Privacy and Electronic Communications (EC Directive) Regulations 2003) implement the EU's ePrivacy Directive (Directive 2002/58/EC) and set out privacy rights relating to electronic communications
  - Director liabilities in respect of consent

- In January 2017, the EU proposed a new ePR (Regulation on Privacy and Electronic Communications) as part of its digital single market strategy.

- The ePR will replace the 2002 ePrivacy Directive (the 'cookies law') and all member state laws that implement it – including the UK's PECR (Privacy and Electronic Communications (EU Directive) Regulations 2003).

- The ePR has been designed to complement the GDPR by providing specific rules *"regarding the protection of fundamental rights and freedoms of natural and legal persons in the provision and use of electronic communications services".*

The EU Cyber Security Act

- The EU Cyber Security Act aims to establish an EU framework for cybersecurity certification, boosting the cybersecurity of digital products and services in Europe.

- The Council has to formally approve the Act, resulting in this new EU Regulation entering into force 20 days after its publication in the Official Journal of the European Union.

- **The Cyber Security Act:**
  - Strengthens the ENISA by granting to the agency a permanent mandate;
  - Enhances the role ENISA plays in supporting EU to achieve a common and high level cybersecurity;
  - Establishes the first EU-wide cybersecurity certification framework to ensure a common cybersecurity certification approach in the European internal market;
  - Aims to improves cybersecurity in a broad range of digital products (e.g. Internet of Things) and services.

Payment Services Directive (PSD2)

- Payment Services Directive (PSD2) was introduced in January 2019 and aims to reduce fraud by introducing substantial changes to processes and technology
- Challenges on how to support “open banking” and share customer information to ensure better tech-based products and services that support the customer, while remaining compliant with GDPR/DPA
- High level of verification for most online payments above €30, known as Strong Customer Authentication, are set to come into force in September.
- It requires retailers, banks and payment groups to fundamentally restructure their payment system.
- Intersects with existing PCI DSS obligations.

THE IMPACT OF CYBER SECURITY LEGISLATION AND REGULATIONS ON KEY COMMERCIAL SECTORS

Regulation & its impact on commercial sectors

Healthcare Sector
- GDPR & DPA 2018
- NIS Directive
- PECR
- PSD2, PCI DSS

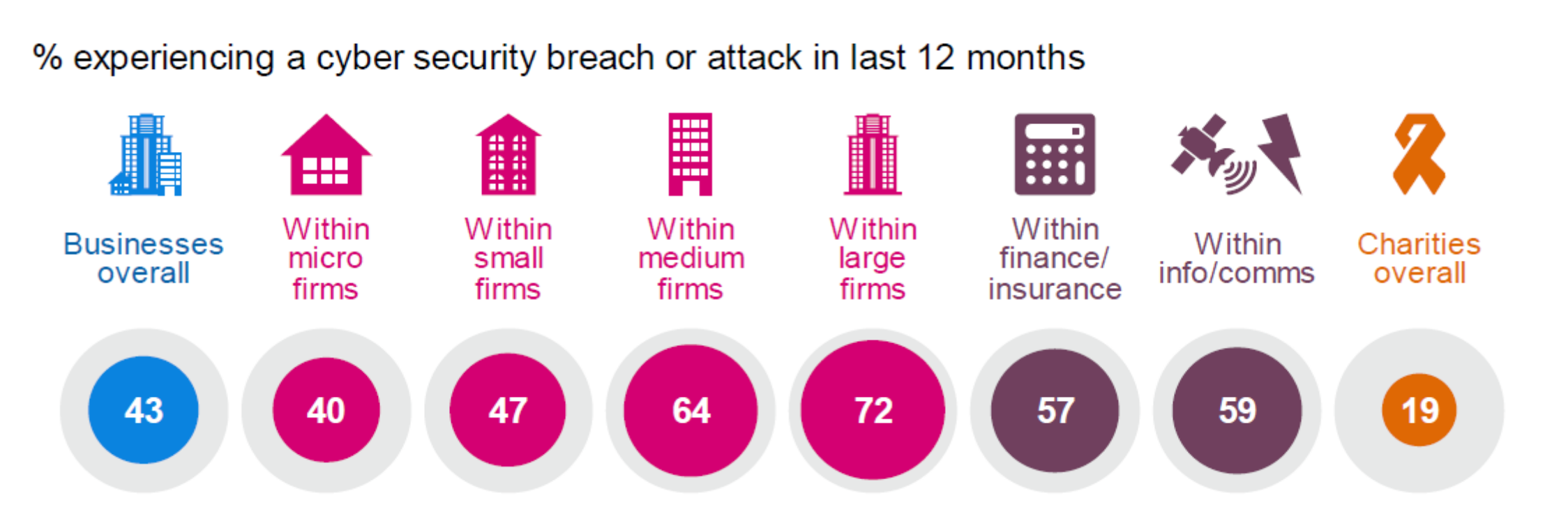
Finance Sector
- GDPR & DPA 2018
- PSD2, PCI DSS
- PECR

Public Sector
- GDPR & DPA 2018
- NIS Directive
- PECR
- PSD2, PCI DSS

Retail, food, travel, hospitality and leisure sectors
- GDPR & DPA 2018
- PSD2, PCI DSS
- PECR

CERTIFICATIONS AND CYBER RESILIENCE

Why is cyber resilience so important?

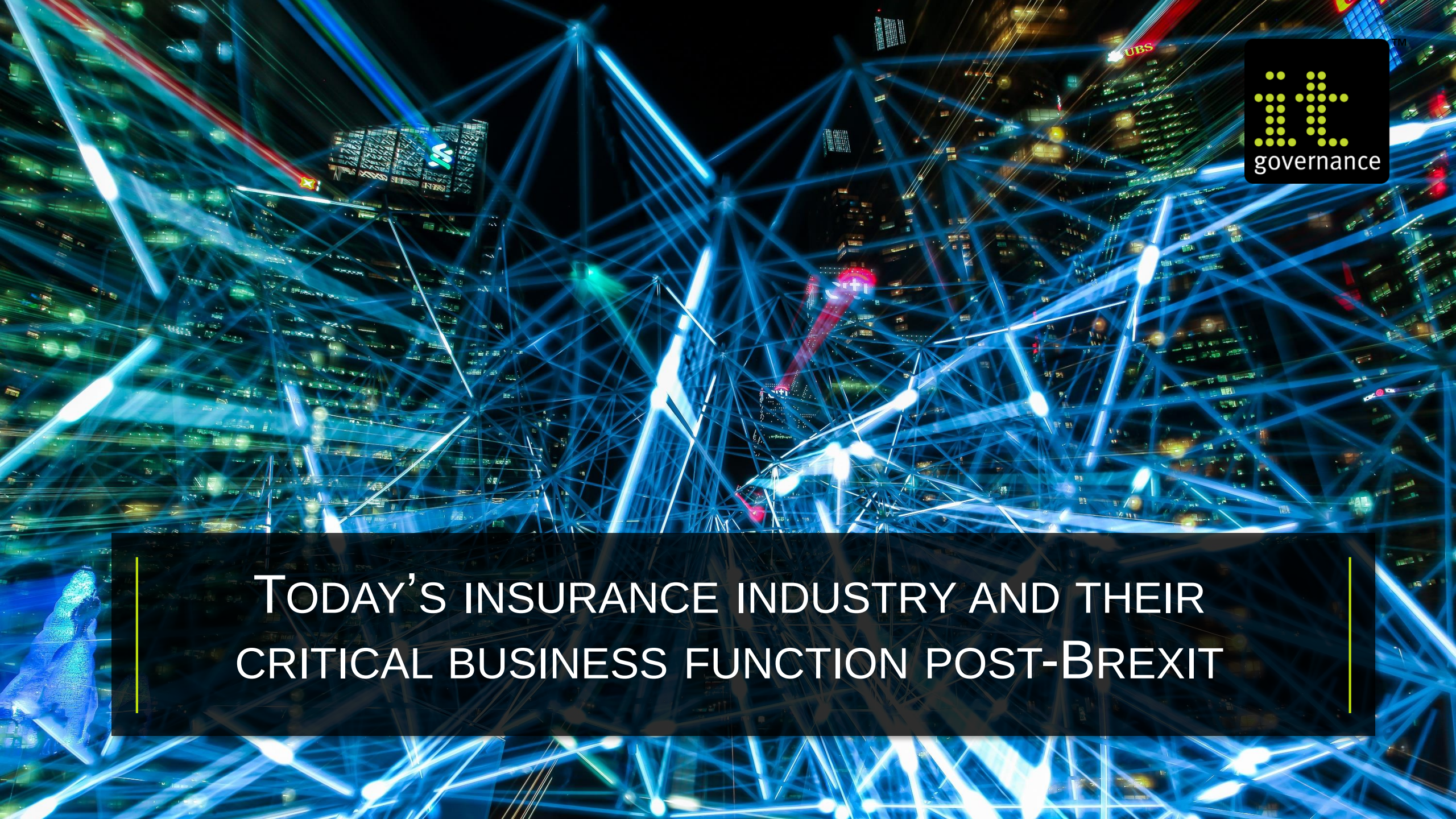


Sophistication of mal-actors, prevalence of multi-vector, multi-layered attacks

Source: DCMS 2018 Cyber Security Breaches Survey

Impacts

- **Financial**
  - Fines
  - Compensation/legal actions
  - Forensic investigations
  - Lost revenue
  - Additional Resource (people, systems) needed to recover
  - Legal Counsel
- **Reputational**
  - Loss of trust with customers (Talk Talk is a good example)
  - Impact on share price
  - Impact on ability to achieve investor funding
- **Commercial**
  - Loss of intellectual property/competitive advantage
- **Operational (NHS –Wannacry)**



Today's insurance industry and their critical business function post-Brexit

The insurance industry & cyber crime

- The FCA made clear that their penalties cannot be covered by insurance - not necessarily the case for the ICO.
- Insurers forced to deal with this issue on a case by case basis, which is unsatisfactory for both the insured and the insurer.
- In the UK, for example, cover cannot generally be obtained for fines imposed for criminal or quasi-criminal conduct for public policy reasons.
- UK Information Commissioner's Office (ICO): "***nothing in the GDPR which either permits or prohibits insurance coverage for regulatory fines"***
- The insurance industry should actively help clients improve cyber security by endorsing basic certifications such as Cyber Essentials and ISO 27001, the global best-practice for information security management systems (ISMS).
- Should a £15k cyber insurance premium really provide £1 million in cover without hard evidence of board-driven cyber security good practice?

The insurance industry: A no-deal Brexit

- UK insurers and intermediaries wouldn’t be able to passport their UK authorisations across Europe (and European insurers wouldn’t be able to passport into the UK).
- UK insurers and reinsurers might be unable to cover risks or pay claims (including policies underwritten before Brexit), and would be subject to third country regimes applying in each EU member state.
- European insurers and intermediaries could be committing criminal offences if they continue to operate in the UK without having entered the UK Temporary Permissions regime (TPR) or the Financial Services Contracts Regime (FSCR).
- Something of a nightmare for UK organisations operating across the EU, dealing with borderless cyber crime.

The operational leadership offered to industry leaders by the government and its impact on safeguarding businesses.

UK Government and cyber security

- The UK Government **sanctioned £22million to improve cyber security operations** in the UK and invest in specialist operations centres.
  - The UK and NATO members to recognise offensive cyber as central to modern warfare.
  - New cyber centres to allow the Army and Defence to transform how they use data.
- Government has long encouraged insurance industry to use certifications to offer innovative cyber insurance products.
- **UK Government initiatives**
  - **Cyber Essentials** is a Government-backed, industry-supported certification scheme to help organisations protect themselves against common online threats.
  - **The National Cyber Security Centre (NCSC)** UK Government organisation that provides advice and support for the public and private sector in how to avoid computer security threats. Based in London, it became operational in October 2016, & is part of GCHQ.
  - CiSP– enables organisations to share information in real time about threats.
- **But our own cyber security is in our own hands!**

How to get in touch

Visit our website
https://www.itgovernance.eu/en-ie

Email us
servicecentre@itgovernance.eu

Call us at
+353 (0) 1 518 0150

Speak to an Expert

Join us on LinkedIn
/company/it-governance

Follow us on Twitter
/itgovernance

Like us on Facebook
/ITGovernanceLtd

Questions

Protect • Comply • Thrive