Balancing Act – Cloud Benefits vs Cloud Security

The cloud is in the mainstream. IT on-premise (traditional IT infrastructure at the user) is migrating in-cloud and providing attractive benefits like provisioning flexibility, access to new services, assisting digital transformation, speed of deployment and cost efficiencies. But business operates in an increasingly intrusive and regulatory environment that emphasises the criticality of data security, sovereignty, residency, privacy and rights. Successfully migrating IT workloads to the cloud means effectively managing these 'legals' to secure the benefits.

A central feature of this transformational change is the epic migration now well underway in enterprise (large organisation) computing from on-premise to in-cloud, where the cloud's share of enterprise IT is forecast to rise from around 10% today to just under 50% by 2026. The development of the enterprise cloud is as significant as the migration of electricity generation out of the factory to the UK National Grid in the 1930s but with many more facets, as each component of IT infrastructure – power, compute, network, memory, storage and software – gets the cloud's 'as a service' treatment.

As enterprise cloud uptake increases, so do cybersecurity risks and threats to the organisation. The UK's National Cyber Security Centre ('**NCSC**', part of GCHQ) recognises that from a security perspective using a Cloud Service Provider ('**CSP**') who has made the 'right security investments'[1] may offer a number of advantages - the large CSPs, with many thousands of security professionals, may well in fact offer better security than an equivalent on-premise installation. However, cloud security is a major part of perceived cybersecurity risks and threats and, as the NCSC noted in its 2017-2018 report, '*the cyber threat to UK business*'[2] (on page 26):

> "[o]nly 40% of all data stored in the cloud is access secured, although the majority of companies report they are concerned about encryption and security of data in the cloud. As more organisations decide to move data to the cloud (including confidential or sensitive information) it will become a tempting target for a range of cyber criminals. They will take advantage of the fact that many businesses put too much faith in the cloud providers and don't stipulate how and where their data is stored."

Organisations are therefore establishing cloud security, compliance and governance frameworks to manage the range of cloud security duties that apply to them and to assess, advise on and assist in managing the risks that are involved. The start point here is a checklist of the sources cloud security duties that may apply to the enterprise. These obligations are diverse and increasingly far-reaching, and will vary by industry sector. The enterprise in the cloud will need to consider not only its own regulatory duties but also those of its customers and supply chains, as well as other generally applicable information security obligations. Enterprises will also need to consider multiple (and potentially conflicting) cloud security obligations across their international operations. These duties break down into four headings:

- regulatory duties:
  - applicable sector specific regulatory duties;
  - generally applicable security and data regulatory duties like data protection, sovereignty, residency and network and information systems security;
  - other generally applicable business regulation like Companies Act directors' duties requirements, etc;
- non-contractual civil law duties:

[1] '*Brightening the outlook for security in the cloud*', NCSC, 26 September 2017, https://www.ncsc.gov.uk/blog-post/brightening-outlook-security-cloud

[2] https://www.ncsc.gov.uk/cyberthreat

  - negligence – where the duty to take 'appropriate technical and organisational measures' to keep data secure in the cloud is emerging as the cybersecurity yardstick by which the normal tort/negligence duty to 'take reasonable care' looks likely to be measured;
  - other civil liability including breach of confidence, copyright, fiduciary or statutory duty, misuse of private information, conversion and trespass;

- contractual duties - between:
  - the CSP and the enterprise;
  - the CSP and its supply chain;
  - the enterprise and its customers; and
  - the enterprise and its supply chain; and

- internal policies and procedures applicable to staff and contractors, including:
  - the range of GDPR policies, procedures and documentation to demonstrate GDPR compliance;
  - training and awareness;
  - duties of confidentiality;
  - device and password controls; and
  - vulnerability assessment/penetration testing.

As with GDPR, you can't just paper your way to cloud and data security compliance and organisations are increasingly developing their own cloud security best practices. There is an increasing array of best practice guidance available, from the CSP community and the public sector/enterprise user community. A good example from the use side is the NCSC's 14 cloud security principles[3], which drill down to the practical detail in a comprehensive set of 14 principles from protecting data in transit through asset protection; separation; governance; security of operations, personnel, development, supply chain, customer management and service administration; to identity; authentication; external interface protection and audit.

An important element of this structured approach to cloud security is showing how the CSP can provide assurance that it will meet its security commitments. The NCSC paper '*having confidence in cyber security*'[4] explains the ways in which cloud buyers can determine and demonstrate compliance with the cloud security principles. These include CSP assertion, CSP contractual commitment, third-party certification, independent testing or a mix of one or more of these. Here, the combination of [contractual commitment] + [accredited standards certification] + [reserving the right to carry out independent testing] is emerging as market practice.

Enterprise cloud migration is set to gather pace in coming months and years, bringing a wide range of IT benefits to large organisations. As we have seen recently with GDPR, security is in the public eye, and legal duties to keep cloud data secure are becoming more onerous. Balancing cloud benefits and security duties is therefore a critical success factor for organisations in their cloud operations. Ensuring cloud security – the mix of legal, technical, operational and governance measures to achieve a desired information security outcome – is moving centre stage as enterprises shift their computing workloads 'off prem'. Putting in place effective cloud security governance frameworks, and the policies procedures and processes that underpin them, is becoming indispensable.

Richard Kemp, Kemp IT Law
June 2018

---

[3] The NCSC has published a suite of helpful cloud security documents: (i) '*Introduction - Understanding Cloud Security*' - https://www.ncsc.gov.uk/guidance/introduction-understanding-cloud-security; (ii) '*Introduction to Risk Management for Cyber Security Guidance*' - https://www.ncsc.gov.uk/guidance/introduction-risk-management-cyber-security-guidance; and (iii) '*Implementing the Cloud Security Principles*' - https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles

[4] https://www.ncsc.gov.uk/guidance/how-confident-can-you-be-cloud-security