Information
Security
Forum

Driving out the seven deadly sins of cloud computing

If you haven't already implemented cloud computing in your organisation, it's a safe bet that someone is already thinking about doing so. It's possible that cloud computing services are already being used 'under the radar'.

Cloud computing offers many benefits, especially in driving down costs and boosting efficiency. However as you roll out cloud services, it's vital to ensure that your business is protected and not exposed to threats to your information security, integrity, availability and confidentiality.

The Information Security Forum (ISF) report – Securing cloud computing: addressing the seven deadly sins – helps organisations develop practical solutions to implementing cloud services safely and securely.

Based on insight from the ISF's global Membership, the report outlines and addresses the 'seven deadly sins' that you should avoid when implementing cloud services:

1. **Ignorance** – little or no management knowledge or approval
2. **Ambiguity** – contracts are agreed without authorisation, review or security requirements
3. **Doubt** – little or no assurance regarding providers' security arrangements
4. **Trespass** – failure to consider the legality of placing data in the cloud
5. **Disorder** – failure to implement proper management of the classification, storage and destruction of data
6. **Conceit** – belief that enterprise infrastructure is ready for the cloud when it's not
7. **Complacency** – assuming 24/7 service availability.

The report, backed by the wide range of related tools and materials available exclusively to ISF Members, helps get organisations fully up to speed in their preparations for the cloud.

The seven deadly sins of cloud computing
... and how to tackle them

Using the seven deadly sins as a framework, the ISF has developed a business-focused approach not only to 'fighting the fires' of *ad hoc*, unplanned implementation of cloud services, but also to adopting a holistic, structured program for ensuring security and cost-efficiency.

This approach is summarised here, while the full report – available only to ISF Members – offers practical guidance in the form of a checklist of actions and a set of common baseline arrangements that organisations can use to secure cloud services.

1 Ignorance

- **SIN** – cloud computing has been implemented around the organisation without the knowledge or approval of either senior management or the IT department.
- **ISSUES** – uncontrolled implementation of cloud services by proxy goes undetected and with little or no understanding of the potential information security risks.
- **ACTION** – implement a purchasing policy for cloud services that requires an information security risk assessment, as well as technology to help identify any cloud service deployments automatically.

2 Ambiguity

- **SIN** – contracts with external cloud service providers are made with little or no attention to the need for authorisation, review or security specifications.
- **ISSUES** – cloud services are implemented without risks being identified and without the identities of all parties associated with the contract being specified, and included in the contract.
- **ACTION** – ensure cloud service providers identify all associated parties and are subject to formal risk assessment to determine any security requirements that should be included in the contract.

3 Doubt

- **SIN** – little or no assurance is gained regarding the cloud provider's security arrangements around how they will protect the organisation's information.
- **ISSUES** – there is poor assessment, monitoring and reporting of cloud providers' security arrangements, combined with difficulty invoking the right to audit.
- **ACTION** – cloud service providers should provide details of their information security architecture, security model, security testing, certifications and independent security audits. Organisations should negotiate the right to audit or implement real-time monitoring to provide assurance.

4 Trespass

- **SIN** – there is no appreciation that putting data in the cloud may be illegal.
- **ISSUES** – by storing data in unknown locations, organisations may be in breach of privacy legislation and data controller obligations.
- **ACTION** – organisations should specify approved storage locations, and arrange appropriate controls to protect data in line with privacy legislation.

5 Disorder

- **SIN** – information placed in the cloud is not classified correctly, stored appropriately or destroyed completely.
- **ISSUES** – inappropriate data ends up being stored on third parties' systems, without formalised access control procedures. For highly regulated industries, it becomes difficult to identify and prove what users are doing.
- **ACTION** – organisations should classify and assess data before it is moved to the cloud, and should ensure that access control procedures deliver the level of assurance required.

6 Conceit

- **SIN** – there is no enterprise-wide infrastructure to support secure use of cloud services, as is the case with internal IT systems.
- **ISSUES** – there is no corporate security architecture defined for cloud services, and no standard approach to identity and access management. What is more, the security of organisations' encryption solutions may be compromised as keys are also stored in the cloud provider's system.
- **ACTION** – organisations need to develop a corporate security architecture for cloud services that sets out their usage, integration with standard services like identity and access management, and security features like encryption.

7 Complacency

- **SIN** – purchasers of cloud services assume they will have full availability, although experience shows that a variety of incidents can, and do, cause cloud outages.
- **ISSUES** – reliance on a single network, such as the Internet, puts critical services at risk, especially if there are no business continuity or disaster recovery plans at the cloud service provider. In addition, eDiscovery orders against the organisation may result in cloud services becoming unavailable, while forensic investigations may be extremely difficult to conduct.
- **ACTION** – organisations should ensure the cloud provider's business continuity and disaster recovery plans – and their availability service level agreements – satisfy their requirements. They should consider the effect of eDiscovery requests on availability and confidentiality, and make alternative arrangements if required.

A practical, holistic approach

As well as tackling the seven deadly sins of cloud service implementation individually, organisations need to take a broader, holistic view to ensure that all aspects of security are addressed.

Experience from outsourcing – and specifically IT outsourcing – has demonstrated the need for a consistent approach to areas such as supplier selection, contracting, monitoring and information security. However, this experience is often ignored and there is no consistent approach to assessing, purchasing and monitoring cloud services.

The ISF recommends that cloud service providers should be treated like any other external supplier such as an outsourcer or offshore outsourcer, and should be covered by the same form of contract. To assist in this, the ISF has developed a four-step approach to working with external suppliers, which provides a consistent set of activities that can equally be applied to cloud service providers:

Step 1 – identify and classify third parties
Step 2 – agree third-party security
Step 3 – validate third-party security
Step 4 – agree termination terms.

In addition, the ISF is now offering a range of training and implementation guidance programmes to assist in rolling out cloud services securely.

Organisations cannot afford to delay getting to grips with the information security implications of cloud computing services: users are signing up to new cloud services daily. The ISF can help organisations move quickly to develop practical, business-oriented solutions to this challenge.

About the ISF

Founded in 1989, the Information Security Forum is an independent, not-for-profit association of leading organisations from around the world. It is dedicated to investigating, clarifying and resolving key issues in information security and developing best practice methodologies, processes and solutions that meet the business needs of its Members.

ISF Members benefit from harnessing and sharing in-depth knowledge and practical experience drawn from within their organisations and developed through an extensive research and work program. The ISF provides a confidential forum and framework, which ensures that Members adopt leading-edge information security strategies and solutions. And by working together, Members avoid the major expenditure required to reach the same goals on their own.

Contact

For further information contact:
Steve Durbin
Tel: +44 (0)20 7213 1745
Fax: +44(0)20 7213 4813
E-mail: steve.durbin@securityforum.org
Web: www.securityforum.org

Disclaimer

This document has been published to provide general information only. It is not intended to provide advice of any kind. Neither the Information Security Forum nor the Information Security Forum Limited accept any responsibility for the consequences of any use you make of the information contained in this document.

Reference: ISF 11 CC (Marketing)