Hex Security Limited

T +44 (0)1432 800440
E info@hexsecurity.co.uk

White Paper

DEMYSTIFYING CLOUD SECURITY

CLOUD SECURITY AND PRIVACY WHITE PAPER

HEX SECURITY
EXPERT INFORMATION ASSURANCE CONSULTANCY

The Cloud

Making the transition to cloud-based services can deliver greater flexibility, agility and cost savings. Resources are available on-demand and can be rapidly provisioned with short-term contracts and simple charges. What a Great Idea!!

The cloud computing model introduces both opportunities and challenges in a centralised multi-tenant and multi-access environment. Company information can be accessed at any time, from anywhere, and from any device. Businesses can take advantage of scalable, flexible and optimised cloud-based services providing opportunities for cost reduction and improved efficiencies. From a security perspective cloud-based defences can benefit from more robust security controls and can offer significant potential to improve overall security and resilience through focused security investment by the cloud service providers. However the concentration of resources and customer data presents a very attractive target to attackers and a compromise of a cloud service provider could have significant impact on the data and reputation of multiple customers. It is essential that cloud customers are confident in the cloud services they procure and understand the security threats, risks and their own security responsibilities.

Cloud-Adoption Strategies

Organisations must understand where they can maximise the benefits offered by cloud computing and minimise any associated impacts. This will be driven by their business goals to develop coherent cloud-adoption strategies to ensure the best use of cloud-based services. Identifying all relevant requirements will help evaluate cloud-service offerings and identify the most suitable applications or information types for cloud deployment and migration.

What about Security Risks & Threats?

There are numerous security risks related to the shared, on-demand nature of cloud computing. This is a global threat as cloud services can potentially be accessed, or attacked, from anywhere in the world. Risks need to be understood in relation to business opportunities to ensure they can be managed to acceptable levels. This white paper provides greater awareness about cloud security and privacy concerns outlining six simple steps to help protect your cloud data and use of cloud services.

Cloud Computing

NIST SP 800-145 defines the key aspects of cloud computing including five essential characteristics, three service models and four deployment models which can deliver a geographically dispersed cloud ecosystem of services.

The cloud is extending the traditional enterprise architecture offering additional services and resources that can be quickly deployed and easily scaled. There are a number of benefits such as Operational Expenditure (OPEX) versus Capital Expenditure (CAPEX) and the ability to choose from an extensive set of services to meet an organisation's needs. However the diverse range of offerings can often result in a complex set of services across a number of locations, boundaries and suppliers. The security of an integrated cloud service architecture needs to be closely managed and controlled to ensure that it delivers both the business and security benefits.

Cloud Security Risks

Different cloud architectures and services will attract different threats and levels of risk. Cloud customers must understand the risks of using cloud computing in the context of their own business environment and risk appetite.

DATA PROTECTION

Legal and Privacy Concerns

Many cloud providers operate across different geographic locations and jurisdiction boundaries. Data may be stored or transferred outside of the EU which may result in privacy concerns and introduce legal non-compliance risks. Cloud customers remain responsible as “Data Controllers” to ensure that personal information is handled and processed correctly by cloud providers as “Data Processors”.

MALICIOUS INSIDER

Unrestricted Access and Control

The risks from a malicious insider are amplified in the cloud context where privileged personnel could have a considerable impact on multi-tenants. The levels of access could enable unrestricted access to customer data and complete control of cloud services with little risk of detection. Verify the background checks, monitoring regime and access controls applied by cloud providers.

LOSS OF GOVERNANCE

Gaps in Security Controls

Outsourcing security responsibilities to cloud providers does offer the economies of security scale but this does not remove security responsibilities from cloud customers. Clear demarcation points need to be agreed to ensure that there are no assumptions regarding responsibilities and to reduce the risk of security control gaps in the end-to-end customer architecture.

CLOUD VULNERABILITIES

Compromise of Cloud Services

Cloud services may be exposed to technical vulnerabilities that could increase the risk of compromise including insecure interfaces or APIs, isolation failures and account/service hijacking. Attacks that exploit previously unknown vulnerabilities are constantly emerging and cloud customers must ensure that their cloud providers actively monitor and perform vulnerability scans and penetration testing.

Cloud Security Risks Continued

DDOS ATTACKS

Loss of Service Availability

Cloud services could become targets of Denial of Service (DOS) or Distributed Denial of Service (DDOS) attacks which could severely impact the uptime and availability of cloud services for multiple customers. Cloud customers need to ensure that adequate DOS/DDOS protection is provided by their cloud providers to protect service delivery for end-users and consumers.

DATA LEAKAGE

Data Loss or Compromise

An essential characteristic of cloud computing is broad network access where services can be accessed remotely, and information can be replicated and stored over a distributed shared cloud architecture. To protect data from compromise cloud customers should ensure that network links and stored data are secured (encrypted) to reduce the risk of data leakage.

CUSTOMER SYSTEMS

Compromised Assets

Cloud customers will consume cloud services through the integration of existing systems, services and end-user devices. These will be authorised to access cloud services but could pose a risk to customer data if inadequate security controls are applied. Certain security responsibilities can be outsourced but customers must ensure that they operate securely and protect their own assets from compromise.

DISASTERS

Inadequate Resilience or Redundancy

Cloud customers should ensure services being delivered offer the required levels of redundancy and resilience to maximise availability in the case of disasters. Cloud providers will offer a range of service levels from single site redundancy to multiple site replication and disaster recovery including VM snapshots, backup/recovery objectives and automated failover. A loss of services or data could have a critical impact.

Cloud Security Benefits

Cloud computing can offer a number of security benefits and opportunities which provide strong security arguments for the adoption of cloud services.

Economies of Security Scale

Focused security investment by CPs

Cloud providers (CPs) should place security at the top of their delivery agenda and invest heavily in ensuring that their services remain, and continue to remain, secure and resilient from a range of attacks. Cloud customers can benefit from this on-going security investment delivering "economies of security scale" for multiple customers.

Hardened Services

Pre-hardened, patched and tested services

Cloud customers can benefit from pre-hardened, patched and security optimised cloud services which have been developed and security tested by the cloud provider. Cloud providers should perform regular vulnerability scanning and penetration testing activities to verify and maintain the security of their services.

Protective Monitoring

24/7/365 Security Operation Centres (SOCs)

Cloud providers can perform real-time monitoring from centralised 24/7 Security Operation Centres to identify intrusions or attempted intrusions using Security Information and Event Management (SIEM) tools from multiple event collection sources. This can provide immediate incident investigation, management and mitigations as a result of attacks.

Physical Security

Highly Resilience, Physically Secure DCs

Multiple highly secure and resilient data centres (DCs) can be used to physically host and protect cloud provider equipment with multi-levels of perimiterisation and physical access controls including secure fencing, vehicle checkpoints, CCTV, alarms, 24/7 guards, patrols, man-traps, swipe, biometrics, redundant power and communications.

G-Cloud

The Government Cloud (G-Cloud) Framework and Digital Marketplace provide access to a range of cloud-based services for UK Public Sector organisations. They offer a simplified way to buy and sell digital services within the Public Sector.

The New Security Approach to G-Cloud

Following the introduction of the Government Security Classification Policy (GSCP) on the 2nd April 2014, Government Digital Service (GDS) advised that it was changing the security assurance process for G-Cloud services and that in most cases Pan Government Accreditation (PGA) was no longer required. The new security approach will require G-Cloud providers to make appropriate security assertions to a set of questions derived from CESG's 14 Cloud Security Principles. This will allow Public Sector organisations to assess and review the security assertion claims made by G-Cloud providers but it is important for buyers to ensure that these claims are backed up with independent evidence. This could include existing PGA or HMG accreditation, ISO27001 certification or other recognised assurance schemes.

- Data in transit protection
- Asset protection and resilience
- Separation between consumers
- Governance framework
- Operational security
- Personnel security
- Secure development
- Supply chain security
- Secure consumer management
- Identity and authentication
- External interface protection
- Secure service administration
- Audit information provision to consumers
- Secure use of the service by the consumer

Simple Steps

Cloud customers must ensure that their data is protected. Aspects of security responsibilities can be outsourced to cloud service providers but customers ultimately remain accountable and must apply due diligence.

Step 1

Choose a Trusted Cloud Provider.

Not all cloud service providers are created equally and cloud customers should ensure that security claims or assertions are backed up with evidence such as independent verification and assurance. The scope and demarcation points between the cloud service provider and cloud customer needs to be agreed to understand the allocation of security responsibilities.

- ISO27001, ISO22301
- SSAE16, ISAE32, PCI-DSS
- DPA Compliance
- HMG Accreditation
- G-Cloud & PSN PGA
- CHECK / CREST Testing

Step 2

Use a Checklist.

Cloud customers can use a checklist of security requirements or questions to obtain responses from cloud service providers. The checklist could include physical, legal, policy and technical requirements associated with customer security needs. Responses can be assessed from multiple cloud providers to select the most appropriate services, or combination of services.

- Security Requirements
- Security Checklist
- Compare Providers
- Assess Compliance
- Assess Risks
- Determine Impacts
- Obtain Assurance
- Select Services

Step 3

Protect Personal Information.

Personal and sensitive personal information must be protected and cloud customers must comply with data protection and privacy laws. The advice from the Information Commissioner's Office (ICO) is that cloud customers should request satisfactory responses to a Data Protection Act checklist from cloud providers. If this is not provided the recommendation to customers is to seek alternative providers.

- Protect Privacy
- Comply with UK/EU Laws
- Consult ICO if needed
- DPA Checklist
- Verify Responses
- Reject Unsatisfactory
- Seek Alternatives if non-compliant

Simple Steps Continued

Step 4

Use Encryption.

Encryption is a key enabler to protect data-in-transit (network encryption) and data-at-rest (storage encryption). If untrusted or unprotected networks are used without encryption then the confidentiality or integrity of information could be compromised in transit. If the cloud storage or data remains unencrypted then any compromise of the shared storage, or inadequate data deletion could increase the data compromise risks. Cloud customers should understand the encryption options available from cloud providers including any key management services.

- Use Encryption
- Protect Data-in-Transit
- Protect Data-at-Rest
- Identify Options
- Key Management
- Accepted Standards (SSL/TLS, IPSec, AES etc)
- Identify Assurance (FIPS-140, CPA, CAPS etc)

Step 5

Secure End-User Devices.

Modern end-user devices such as laptops, tablets and smartphones provide users with greater flexibility and functionality including access to cloud based services. Compromised endpoints could be used to launch malicious attacks or exfiltrate data. Devices that have access to cloud data should be secured and organisations need to consider controls to minimise the risk and damage that a compromised endpoint can inflict.

- Access Controls
- Identification and Authentication
- Secure End-User Devices
- Use Encryption
- Mobile Device Management
- Mobile App Management
- BYOD/CYOD Policies

Step 6

Operate Securely.

Organisations should recognise and adopt security best practice and ensure that they operate an integrated security culture as components of strategy, process, technology and people improvement. Independent certifications such as Cyber Essentials and ISO27001 could be considered to help verify the robustness of the security practices which includes those applicable to the use of cloud based services.

- Security Culture
- Security Strategy
- Security Technology
- Security Process
- Security Awareness
- Security Verification
- Security Improvement
- Certifications (Cyber Essentials, ISO27001 etc)

Trusted Cloud Provider

Cloud customers must understand their business and security requirements to select a trusted cloud provider that can meet their specific compliance needs.

Reputation

Select a cloud provider with a strong security reputation backed by independent evidence.

Secure

Select a cloud provider that meets your own business and security requirements.

Accredited

Select a cloud provider that has independent certification and accreditation.

Assured

Select a cloud provider who undergoes regular independent vulnerability and penetration testing.

Not all Cloud Providers will apply the same level of security investment to ensure that their cloud services and customers are protected from confidentiality, integrity and availability attacks.

Trusted cloud providers will see security as a market differentiator and will invest heavily in their security controls to give customers the confidence that they implement robust and effective security measures. Proportionate assurance and independent assessments are needed to understand the overall effectiveness of security implementations and to identify opportunities for on-going improvement. Cloud customers should look for trusted cloud providers that can provide independent evidence to validate and demonstrate the robustness of their security practices such as ISO27001, ISO22301, SSAE16/ISAE32 or PCI-DSS certifications. The scope of these assessments should be reviewed to ensure that they cover the range of cloud services being considered. For Public Sector organisations additional assurances and accreditations may be required in support of their own HMG specific requirements, standards and connections. All services should be subject to regular vulnerability scanning and penetration testing to identify and rectify potential weaknesses supported by real-time protective monitoring, intrusion detection and prevention. This could be delivered through a combination of in-house and independent testing services such as those provided by CREST, CHECK or TIGER schemes.

Personal Information

Ensure Personal Information is Protected

Organisations must comply with data protection and privacy laws

Data Controller

Cloud customers must remember that they remain ultimately responsible for their personal information as the registered "Data Controller" and cloud providers will act only as the "Data Processor" in relation to customer data. It is the responsibility of the cloud customer whose data is hosted within a cloud computing environment to maintain compliance with data protection legislation in respect to their personal or sensitive personal information. This includes undertaking and managing registration with the Information Commissioner's Office (ICO) and for conducting any Privacy Impact Assessments (PIAs). Cloud customers must seek evidence from cloud providers that their data will be handled in a lawful way including any data transfers between locations. This can be achieved using a Data Protection Act Checklist for cloud providers to complete.

Legislation

The UK Data Protection Act 1998 provides the strict controls and principles for protecting personal information in the UK:

- Derived from EU Directive 95/46/EC
- Eight Data Protection Principles
- No Transfers Outside EEA (without adequate protection)
- US Safe Habor Privacy Programme
- Model Clauses
- Binding Corporate Rules

Encryption is Key

Encryption is a key component to protect the use of cloud services and to minimise the confidentiality and integrity risks to customer data.

Data at Rest

There are multiple ways to encrypt data-at-rest (storage encryption) including full disk encryption, directory or file level encryption and application level encryption. This provides access to store information only if the associated keys are accessible and may be applied by the cloud customer prior to cloud delivery or by the cloud provider as part of their service. Key management is critical to the effectiveness of any encryption mechanism as any key compromise would impact the protection provided. It is important to note that information will be accessible following the decryption process.

Data in Transit

The aims of data-in-transit (network encryption) is to prevent data being tampered with (integrity) and ensuring that data remains private (confidentiality). This is particularly important where cloud services are accessed over untrusted public bearers (e.g. the Internet). There are a number of common data-in-transit encryption methods that can be employed between cloud customers and cloud providers including TLS/SSL and IPSec VPNs. Ensure access to cloud services are secured over encrypted connections combined with authentication to create protected channels to and from the cloud.

Mobile Device Management

Mobile devices should be securely configured to effectively manage the associated risks to an organisation's enterprise services including those delivered through cloud services. MDM can provide comprehensive security control over all mobile devices.

Mobile Device Management (MDM)
Controls the configuration and protects data on mobile devices with security policies and incident management.

Mobile App Management (MAM)
Manages the deployment, update, approval and removal of commercial and in-house mobile apps.

The combination of Mobile Device Management (MDM) and Mobile Application Management (MAM) can provide an enterprise ready secure mobile device and application management solution.

Many organisations have policies for Choose Your Own Device (CYOD) where mobile devices are owned, issued and managed by the organisation. Some organisations provide staff the flexibility to use their own laptops, smartphones and tablets to conduct business as part of a Bring Your Own Device (BYOD) policy. MDM can support both CYOD and BYOD models to deliver a balance between an enabled mobile user and a securely managed device. Permitting devices where organisations do not have sufficient control can introduce a range of security risks and data protection concerns and organisations need to consider effective Mobile Device Management. MDM solutions allow organisations to manage a variety of mobile device platforms including Apple iOS, Windows 8.x, Samsung and other Android-based devices.

Organisations can manage an inventory of mobile assets to track and apply security policies and restrictions. This includes the ability to locate, block or wipe mobile assets in the event of a potential loss or compromise. MDM can support application blacklisting and whitelisting to manage users' access to applications on their devices. This is supported by Mobile Application Management (MAM) that can provide centralised security and control over custom and third-party mobile apps. This includes app wrapping which allows specific policies to be set for an application or group of applications such as storage encryption requirements and separation/isolation between different apps. The combination of MDM and MAM provides a robust enterprise grade mobility management and security solution and are available as cloud-subscription services.

Cyber Essentials

The Cyber Essentials Scheme is a Government backed initiative that focuses on five key security controls to protect organisations from common Internet based threats to reduce an organisation's vulnerability to attack.

Cyber Essentials
Stage One

Cyber Essentials (Basic) is the entry level certification where organisations self-assess and assert that their systems meet the requirements of the Cyber Essentials Scheme. The self-assessments are independently verified by a Cyber Essentials certification body.

Cyber Essentials +
Stage Two

Cyber Essentials (Plus) offers a higher level of independent assurance where an organisation's systems are tested to verify that they meet the requirements of the Cyber Essentials Scheme. This may include an external vulnerability scan of systems and a security assessment of end-user devices.

Growing Maturity
Integrated

The Cyber Essential Scheme is not intended to be a one-stop certification process and re-certification is required to help it become an integrated part of an organisation's information risk management approach in accordance with the Government's 10 Steps to Cyber Security.

BOUNDARY FIREWALLS AND INTERNET GATEWAYS
SECURE CONFIGURATION
ACCESS CONTROL
MALWARE PROTECTION
PATCH MANAGEMENT

Hex Security Limited

About Us

Hex Security Limited is a Trusted Information Assurance (IA) and Security Company providing specialist consultancy services focused on security certification and accreditation. We are recognised security experts and the experience of our consultants provides customers with the required levels of expertise and knowledge across a diverse range of industries and technologies. Our priority is to help our customers achieve their business goals through the identification and effective management of associated security risks. As a trusted partner, we aim to develop and maintain long term customer relationships delivering on-going commitment and consultancy services.

Our Team

Our team has extensive experience and success in achieving certification and accreditation for commercial organisations, SMEs, HMG departments, MOD, large system integrators and cloud service providers. Our IA and security professionals include ISO27001 and 22301 Auditors, Full CESG Listed Advisor Scheme (CLAS) members, Lead CESG Certified Professionals (CCP), Certified Information Systems Security Professionals (CISSP), Certificate of Cloud Security Knowledge (CCSK) holders, and many more. These qualifications and certifications, coupled with focused security degrees, recognise over 20 years' of IA experience. We are also certified under the UK Cyber Essentials Scheme.