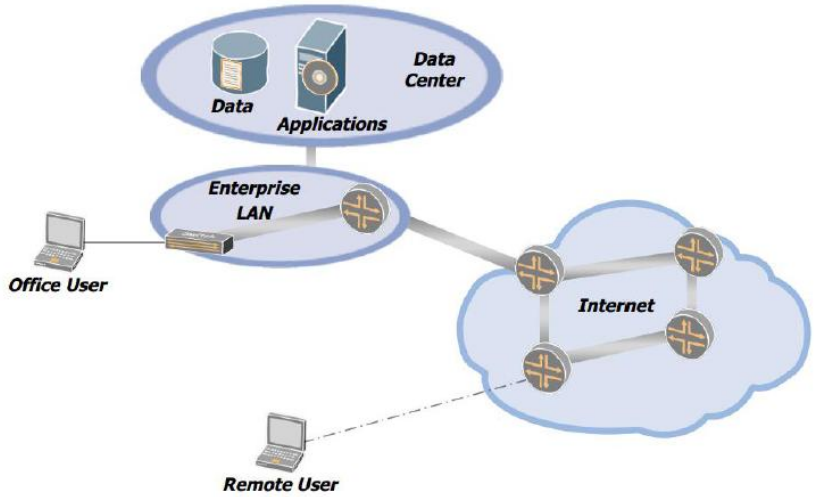
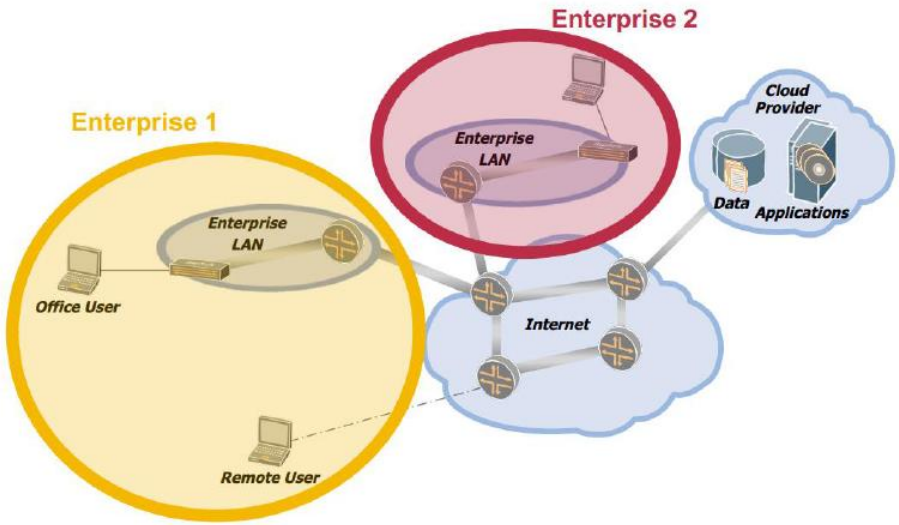
Cloud Security: The Challenges for the Data Centre and IT Environment

www.sdgc.com

Data Centre – Conventional Vs Cloud Modelled



Conventional Data Centre

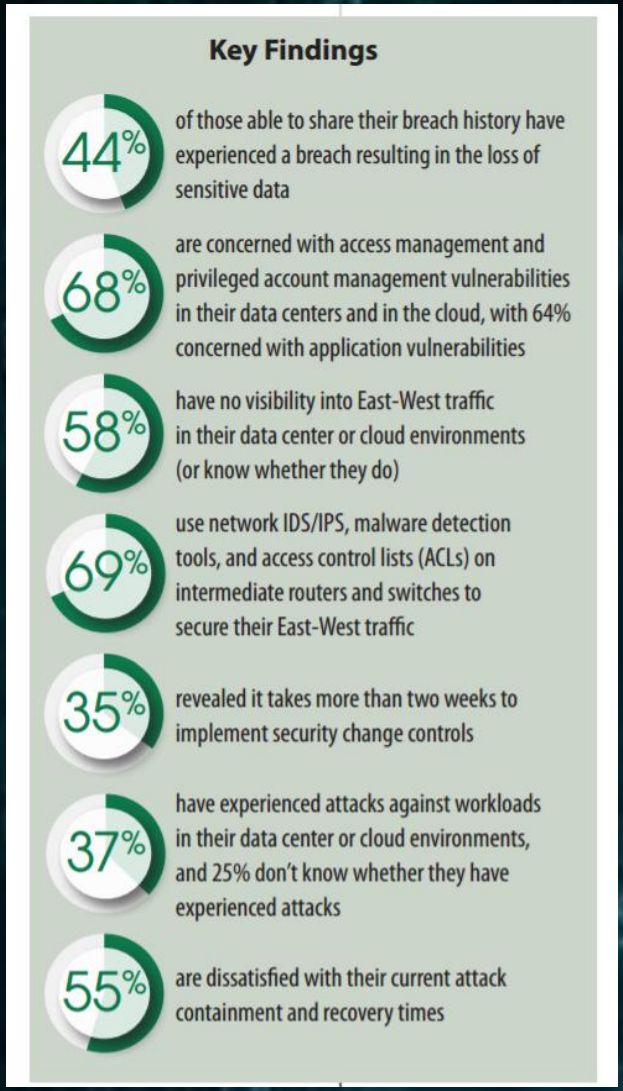


Cloud Modelled Data Centre

The main difference between a cloud modelled data center and a conventional data center is that a cloud modelled one is an off-premise form of computing that stores data on the Internet, whereas a conventional data center refers to on premise hardware that stores data within an organization's local network.

While cloud services are outsourced to third-party cloud providers who perform all updates and ongoing maintenance in a cloud modelled data center, conventional data centers are typically run by an in-house IT department.

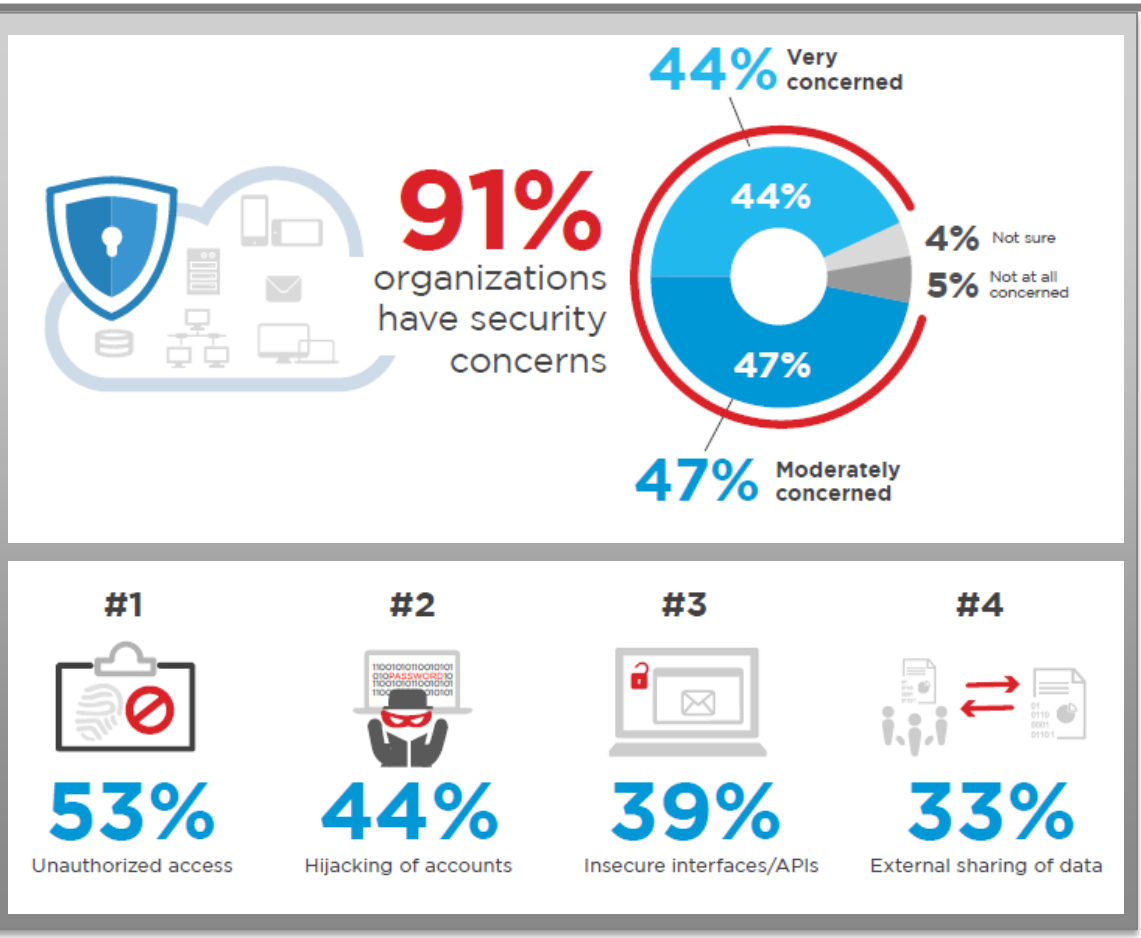
Current Scenario



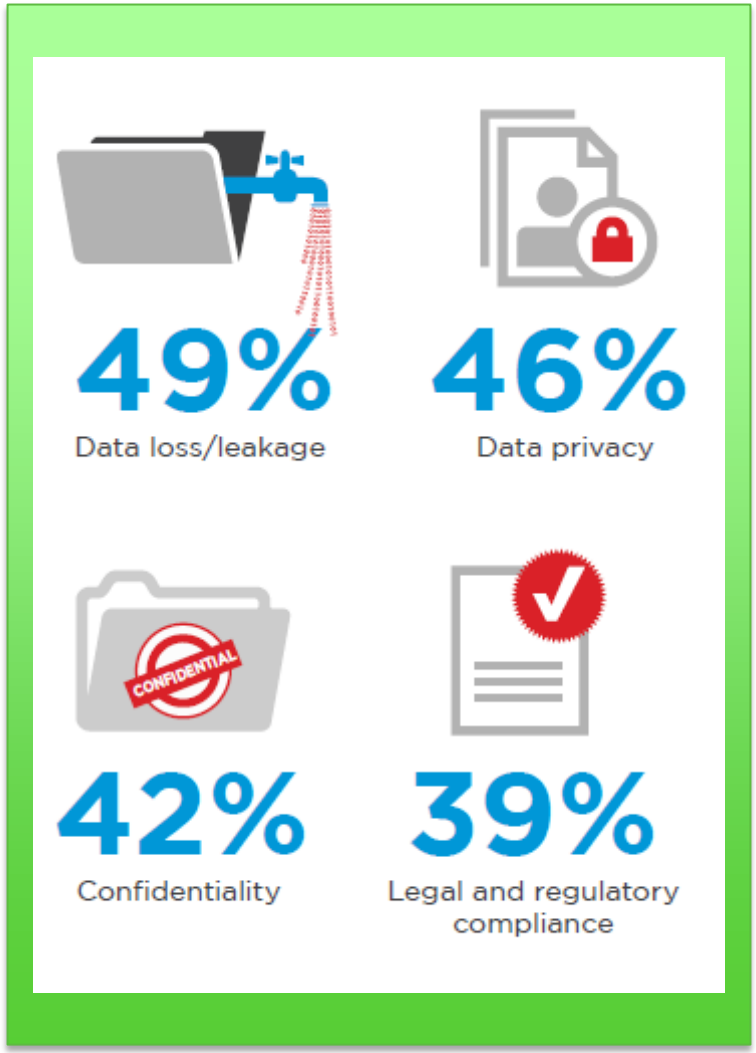
Today, with a variety of architectural options available, corporate data centers have grown enormously as organizations have moved workloads from traditional data center deployments to hybrid cloud infrastructures that can be managed dynamically among internal and cloud-based data centers.

The connections between corporate information systems have become more complex.

Survey Results: Cloud Security 2016



Top Security Threats



Top Security Concerns

Courtesy: Cloudpassage.com

Survey Results: Gartner Report 2016

3 **By 2018, the need to prevent data breaches from public clouds will drive 20% of organizations to develop data security governance programs.**

Recommended Action: Develop an enterprise-wide data security governance (DSG) program. Identify data security policy gaps, develop a roadmap to address the issues and seek cyberinsurance when appropriate.

5 **By 2020, 80% of new deals for cloud-based CASB will be packaged with network firewall, secure web gateway (SWG) and web application firewall (WAF) platforms.**

Recommended Action: While concerns exist about customer migration to the cloud and bundling purchases, companies should assess the application deployment roadmap and decide whether investment is justified.

Data Breaches

Data Loss

System Vulnerabilities

Abuse and Nefarious Use of Cloud Services

Insufficient Identity, Credential and Access Management

Advanced Persistent Threats

Malicious Insiders

Insufficient Due Diligence

Insecure Interfaces and APIs

Account Hijacking

Denial of Service

CLOUD SECURITY CHALLENGES

Courtesy: CSA report 2016 on Cloud Computing Top Threats in 2016

Data Breach & Data Loss

A data breach is an incident in which sensitive, protected or confidential information is released, viewed, stolen or used by an individual who is not authorized to do so. It may involve any kind of information that was not intended for public release like - personal health information, financial information, personally identifiable information (PII), trade secrets and intellectual property.

Cloud providers are highly accessible and the vast amount of data they host makes them an attractive target.

The best protection against data breach is an effective security program. Two important security measures that can help companies stay secure in the cloud are **multifactor authentication and encryption**.

Insufficient Identity, Credential and Access Management

A data center is also physically connected to a local network, which makes it easier to ensure that only those with company-approved credentials and equipment can access stored apps and information

The cloud, however, is accessible by anyone with the proper credentials anywhere that there is an Internet connection.

This opens a wide array of entry and exit points, all of which need to be protected to make sure that data transmitted to and from these points are secure

Insecure Interfaces and APIs

Cloud computing providers expose a set of software user interfaces (UIs) or application programming interfaces (APIs) that customers use to manage and interact with cloud services

From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to circumvent policy.

In addition to security-specific code reviews, rigorous penetration testing becomes a requirement.

Account Hijacking

Cloud solutions add a new threat to the landscape. If an attacker gains access to your credentials, they can eavesdrop on your activities and transactions, manipulate data, return falsified information and redirect your clients to illegitimate sites.

Your account or service instances may become a new base for attackers.

Organizations should look to prohibit the sharing of account credentials among users and services and leverage strong two-factor authentication techniques where possible. All accounts and account activities should be monitored and traceable to a human owner.

Malicious Insiders

A malicious insider, such as a system administrator, can access potentially sensitive information.

From IaaS to PaaS and SaaS, a malicious insider can have increasing levels of access to more critical systems and eventually to data. Systems that depend solely on the cloud service provider (CSP) for security are at greater risk here.

The controls available to limit risk from malicious insiders include **controlling the encryption process and keys, ensuring that the CSP has proper policies; segregating duties; minimizing access by role; and effective logging, monitoring and auditing of administrators' activities.**

Advanced Persistent Threats & Denial of Service

Advanced security threats are now more targeted and stealthy.

They no longer focus on denial of service alone, but on the **valuable data residing in the data center.**

Awareness programs that are regularly reinforced are one of the best defenses against these types of attacks, because many of these vulnerabilities require user intervention or action

System Vulnerabilities

System vulnerabilities are exploitable bugs in programs that attackers can use to infiltrate a computer system for the purpose of stealing data, taking control of the system or disrupting service operations.

While the damage resulting from attacks on system vulnerabilities can be considerable, such attacks can be mitigated with basic IT processes.

Organizations that are highly regulated (e.g. government and financial institutions) need to be capable of handling patching quickly and, when possible, in an automatic recurring fashion. Security management must put in place a threat intelligence function, to fill the gap between the time a vulnerability is announced (known as ‘0-day’), and the time a patch is provided by the vendor.

Insufficient Due Diligence

An organization that rushes to adopt cloud technologies and choose CSPs without performing due diligence exposes itself to a myriad of commercial, financial, technical, legal and compliance risks that jeopardize its success.

The bottom line for enterprises and organizations moving to a cloud technology model is that they must perform extensive due diligence to understand the risks they assume by adopting this technology model and engaging the suppliers who provide it.

Abuse and Nefarious Use of Cloud Services

Poorly secured cloud service deployments, free cloud service trials and fraudulent account sign-ups via payment instrument fraud expose cloud computing models such as IaaS, PaaS, and SaaS to malicious attacks.

A cloud provider must have an incident response framework to address misuse of resources, as well as a means for customers to report abuse originating from a cloud provider. A cloud provider should include relevant controls that allow a customer to monitor the health of their cloud workload.

“The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards”

Reach me at:

Meetali Sharma
meetalisharma81@gmail.com
+91-9971393639