



# ARE THE CLOUDS IN THE CONVERGED CLOUD DARKENING?

Ramesh Munamarty,  
Group Chief Information Officer  
International SOS

# THE DAILY NEWS

[www.dailynews.com](http://www.dailynews.com)

**THE WORLD'S FAVOURITE NEWSPAPER**

**- Since 1879**

Cybercrooks use stolen Vendor ID to hack into system exposing 70 million household records

Bank says their system gets hacked every day. 76 million household records breached

Major US Retailer claims 56 million records breached

80 million health records exposed

Medical records of 26 million patients are embroiled in a major security breach amid warnings that the IT system used by thousands of GPs is not secure.

# THE DAILY NEWS

[www.dailynews.com](http://www.dailynews.com)

THE WORLD'S FAVOURITE NEWSPAPER

- Since 1879



Security breach fears over 26 million NHS patients -2017

**In 2016, there have been 454 data breaches with nearly 12.7 million records exposed. Over 169 million personal records were exposed in 2015, stemming from 781 publicized breaches**

**“In 93% of breaches, attackers take minutes or less to compromise systems.”**

**Only 38% of global organizations feel prepared for a sophisticated cyberattack.”**

**The forecast average loss for a breach of 1,000 records is between \$52,000 and \$87,000.”**

**“80% of analyzed breaches had a financial motive. 68% of funds lost as a result of a cyber attack were declared unrecoverable.””**

**“74 percent of CISOs are concerned about employees stealing sensitive company information”**



# IBM X-FORCE TII



no.203.078

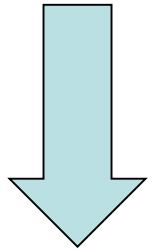
IBM's SECURITY REPORT 2017 - ABYSMAL

- Since 1802

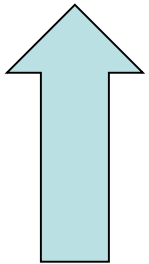
## IS THE FORCE WITH US?

- The number of records compromised grew a historic 566% in 2016 from 600 million to more than 4 billion -- more than the combined total from the two previous years.
- In one case, a single source leaked more than 1.5 billion records [[Yahoo](#) breach].
- In the first three months of 2016, the FBI estimated cybercriminals were paid a reported \$209 million via ransomware. This would put criminals on pace to make nearly \$1 billion from their use of the malware just last year.
- In 2016, many significant breaches related to unstructured data such as email archives, business documents, intellectual property and source code were also compromised.
- The most popular types of malware we observed in 2016 were Android malware, banking Trojans, ransomware offerings and [DDoS-as-a-service](#) vendors.

# Cloud Computing



- Capital Costs
- Operating Costs



- Operations
- BCP/DR
- Efficiency



# Cloud Computing



- Environmental Security – Concentration of Security Threats
- Data Privacy and Security – Transfer of control of data security
- Data Availability and Business Continuity – Loss of Internet Connectivity or Seizure by Law Enforcement Agency can bring business to halt if backup plan does not exist
- Record Retention Requirements – Financial, Litigation hold and preparedness

# Ten Steps to Mitigate Risk

## 1. ENSURE EFFECTIVE GRC PROCESSES EXIST

- Ensure MSA and SLA capture security requirements according to the type of service – IaaS, PaaS, SaaS
- Notification mechanism for breach
- Jurisdictional issue for PII data
- ISO/IEC 27017 [4] - "Code of practice for information security controls based on ISO/IEC 27002 for cloud services"
- ISO/IEC 27018 [5] "Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors"
- Groups such as the Cloud Security Alliance (CSA) provide guidance including provider self assessment, CAI and CCSK



# Ten Steps to Mitigate Risk

## 2. AUDIT OPERATIONAL AND BUSINESS PROCESSES

- Understanding the internal control environment of a cloud service provider
- Access to the corporate audit trail
- Automated and recurring patch management following Change Control procedure
- Common defense-in-depth mechanisms and avoiding sharing account credentials including monitoring of all accounts including service accounts
- Reinforced awareness programs for spear phishing prevent APTs into the network



# Ten Steps to Mitigate Risk

## 3. MANAGE PEOPLE, ROLES AND IDENTITIES

- If you have an IdAM system, integrate it with the cloud vendor
- Can the provider offer delegated admin to administer users?
- Can provider offer Single Sign-on and Sign-off?
- Need Audit control and audit reports
- Does the cloud provider offer MFA, Biometric or other Strong Authentication?
- Does the platform allow fine-grained access control to provide segregation of duties
- Visibility to user actions (e.g. avoid common insider threat- prevent sales person to download all sales contact prior to exit)



# Ten Steps to Mitigate Risk

## 4. ENSURE PROPER DATA PROTECTION

- Create data asset catalog
- Consider all forms of data – structured and unstructured.
- Consider privacy requirements for PII data and avoid contractual breaches
- Apply CIA. Encryption in case of provider storing keys needs caution
- Apply IdAM. Logging, communication and data forensics
- Distribute data, have regular backups and ensure encryption keys are not lost to prevent permanent data loss.
- Harden APIs as they tend to be the most exposed part of system



# Ten Steps to Mitigate Risk

## 5. ENSURE DATA PRIVACY

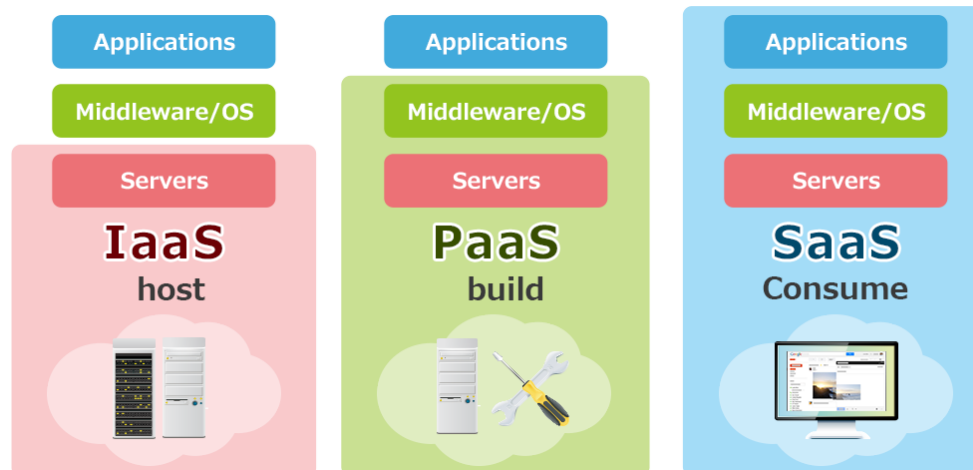
- Responsibility of Data privacy rests with the customer (*the data controller in EU terminology*)
- Most companies operate under some sort of regulatory control of their information (e.g. HIPAA, FERPA, FISMA). Under these mandates, companies must know where their data is, who is able to access it, and how it is being protected.
- Periodically audit provider's adherence to customer's data privacy policies and mechanisms to address via corrective actions



# Ten Steps to Mitigate Risk

## 6. ASSESS SECURITY PROVISIONS

- IaaS - System assurance, testing should be more rigorous than for an on premises application, since the application will reside outside of the customer's security perimeter.
- PaaS - Encryption and key management standards based on data classification. Customer should know how privileged data access.
- SaaS – Customer should understand security for data at rest and in motion and how sensitive data is being handled



# Ten Steps to Mitigate Risk

## 7. ENSURE CLOUD NETWORKS AND CONNECTIONS ARE SECURE

Ensure provider has following:

- Traffic screening – such as to malware ports, published firewall perimeter block list
- Denial of Service protection – cloud providers more prone to DoS and DDoS attacks.


A single vulnerability can comprise the complete cloud.

- IDS/IPS
- Logging and Notification – need network logging and retention policy.  
SLAs for notification.



# Ten Steps to Mitigate Risk

## 8. EVALUATE SECURITY CONTROLS ON PHYSICAL INFRA AND FACILITIES

- Protection against environmental and external threats
  - Control of personnel in secure areas doing malicious acts
  - Supporting utilities should have controls for disruption
  - Proper equipment maintenance
  - Human Resources security
  - Backup and DR procedures
- 
- A red fire extinguisher icon is located in the bottom right corner of the slide. It is a stylized graphic of a fire extinguisher with a red body and a white nozzle, set against a red hexagonal background.



# Ten Steps to Mitigate Risk

## 9. MANAGE SECURITY TERMS IN THE AGREEMENT

- Have clear guidelines for notifications
- Metrics and standards for measuring performance and effectiveness of information security management should be established in advance in the cloud service agreement.
- Certification to a suitable standard like ISO/IEC 27018 is preferable. Otherwise, a data compliance report should be required
- Role clarity for various categories of cloud computing technical architecture – IaaS, PaaS, SaaS



# Ten Steps to Mitigate Risk

## 10. UNDERSTAND SECURITY REQUIREMENTS OF EXIT PROCESS

- None of customer data should reside with provider
- Backups must be retained till agreed upon period before elimination
- Associated event logs and reporting data should be retained and then permanently erased
- Ensure there is no loss or breach of data during exit



## summary

**The clouds are darkening but the following steps can lighten them:**

- 1. Ensure effective GRC processes exist**
- 2. Audit operational and business processes**
- 3. Manage people, roles and identities**
- 4. Ensure proper data protection**
- 5. Ensure Data Privacy**
- 6. Assess Security Provisions**
- 7. Ensure cloud networks and connections are secure**
- 8. Evaluate security controls on physical infra and facilities**
- 9. Manage security terms in the agreement**
- 10. Understand security requirements of exit process**



Contact Information:

Ramesh Munamarty

Group CIO, International SOS

[Ramesh.Munamarty@internationalsos.com](mailto:Ramesh.Munamarty@internationalsos.com)