Can SaaS Ever be Secure?

Helen McLaughlin

OWASP AppSecEU 15
Amsterdam, The Netherlands

Helen McLaughlin, MSc Info Sec

EMEA Information Security Architect at workday.

Over 15 years as a technology professional, with 10 years in Financial Services, Helen has been responsible for delivering software development and integration programmes, as well as managing operations support teams for global business applications.

Trends with Cloud Computing

OWASP AppSecEU 15
Amsterdam, The Netherlands

Consensus that SaaS Adoption is Accelerating

Despite varying forecasts all consultancies and research firms agree adoption of Cloud Computing is accelerating, with these trends:

- IT decision makers increasing spend on Cloud computing
- SaaS will lead growth beyond both IaaS and PaaS
- Cloud computing will become the new delivery model
- Security, Cloud and Mobile are the top 3 focus areas for IT executives in 2015

Gartner

FORRESTER®

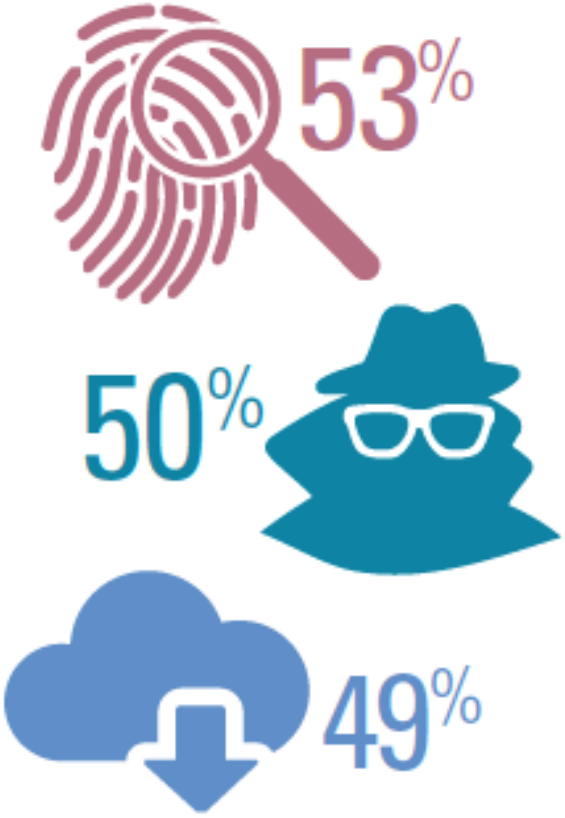
Goldman Sachs

accenture

KPMG

http://www.forbes.com/sites/louiscolumbus/2015/01/24/roundup-of-cloud-computing-forecast estimates-2015/
http://www.kpmginfo.com/EnablingBusinessInTheCloud/downloads/7397-CloudSurvey-Rev1-5-15.pdf

Concerns with Adoption of Cloud Services



Data loss and privacy risks

Risk of intellectual property theft

Impact on IT organization

48% Measuring on ROI

48% High cost of implementation

46% Legal and regulatory compliance

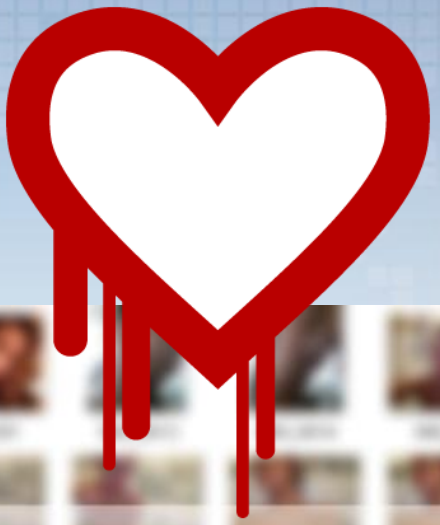
46% Integration with existing architecture

46% Lack of clarity of total cost of ownership

Source: 2014 KPMG Cloud Survey Report

http://www.kpmginfo.com/EnablingBusinessInTheCloud/downloads/7397-CloudSurvey-Rev1-5-15.pdf

Greater Awareness with Executives of Security Risks



OWASP AppSecEU 15
Amsterdam, The Netherlands

Capabilities Sought in Cloud Service Providers

Security

Data privacy

Cost/price

76% Functionality

74% Cost of ownership

74% Ease of integration into existing environment

74% Configurability

67% Additional services offered by provider

Source: 2014 KPMG Cloud Survey Report

http://www.kpmginfo.com/EnablingBusinessInTheCloud/downloads/7397-CloudSurvey-Rev1-5-15.pdf

Are concerns valid?

Data Security and Privacy Challenges are Not New

Consider Business Process Outsourcing, the challenges are neither unique nor new:

- Payroll
- Recruitment
- Accounting
- IT Support Services
- Call Centres

https://privacyassociation.org/media/presentations/12DPC/DPC12_Field_Guide_HO2.pdf

International Transfers of Data are Not New

- Emailing of spreadsheets between office locations, to partners or suppliers or subsidiaries or customers
- Data often needs to transfer across borders, whether hosting the services themselves or with a cloud service provider
- These are not additional or new considerations for a company doing business in the information age

https://privacyassociation.org/media/presentations/12DPC/DPC12_Field_Guide_HO2.pdf

Assurance with SaaS

OWASP AppSecEU 15

Amsterdam, The Netherlands

Regulatory Compliance

- Understand regulatory requirements in your industry and jurisdiction: core business versus office/ shared services
- Understand Privacy Regulation: Data Controller vs Data Processor, who can see and do what from where
- Consult Compliance and Legal Counsel during decision making, contract negotiation and solution design phases
- Be informed about changes in the regulatory landscape to ensure ongoing compliance

Trust but Verify: Independent Audit Reports

- **ISO 27001** - the ISMS to protect information assets from threats whether internal or external, deliberate or accidental
- **SSAE16 SOC-1 & SOC-2/ ISAE3042 Audits** - Auditing standard developed by the American Institute of Certified Public Accountants (AICPA)
- **Safe Harbor** – Commitment to maintain Safe Harbor Certification (EEA & Switzerland) and to comply with **applicable controls** for processing data
- **TRUSTe Cloud Privacy Certification** - Certification demonstrating high standards for data management and privacy for the Service.

Benchmark Providers

- **BITS Shared Assessments**
  - Created by **leading financial institutions, the Big 4** and key **service providers** to evaluate the security controls of vendors
  - Shared Information Gathering (SIG) qu'aire
  - 2,000+ companies across 120 countries annually

- **Cloud Security Alliance (CSA)**
  - Cloud Security Alliance is a non-profit, to promote the use of best practices for security assurance within Cloud Computing
  - CSA STAR Self Assessment

Differentiators of SaaS providers

- Dedicated Security organisation, core business
- Follow best practice and are active with standards bodies
- Secure by design as built for cloud: always on-auditing, encryption, configurable
- Single security model in the application
- Stricter access control for support functions

Changing the Focus of IT

- Agree framework for attestations and assurance through audit between technology layers and providers to demonstrate end to end compliance
- Policies, roles, responsibilities are evolving

Take Aways

- SaaS is here to stay
- Nobody wants and event with data breach
- The challenges are not new
- Understand your requirements from a regulatory and business perspective
- Define your governance and monitoring framework
- Risk assess your SaaS controls frequently
- Review policies, roles and responsibilities