Risks and Rewards in Cloud Adoption

Adrienne Hall
General Manager, Trustworthy Computing
Microsoft Corporation

Microsoft

Vis, Croatia


Awesome docking
Showers
Fabulous Fish dinners
Military History Tour
Gauss

Perspective

Server Proliferation

SIRv1

1990 1994 1998 2002 2003 2004 2006 2008 2009 2010 2012

Internet Tidal Wave

Coordinated Vulnerability Disclosure

Security Intelligence Report

New Release SIRv13 Today

Worldwide Threat Assessment

Infiltration of Supply Chain

Vulnerability trends

Criminal focus on Java and HTML

Exploit trends

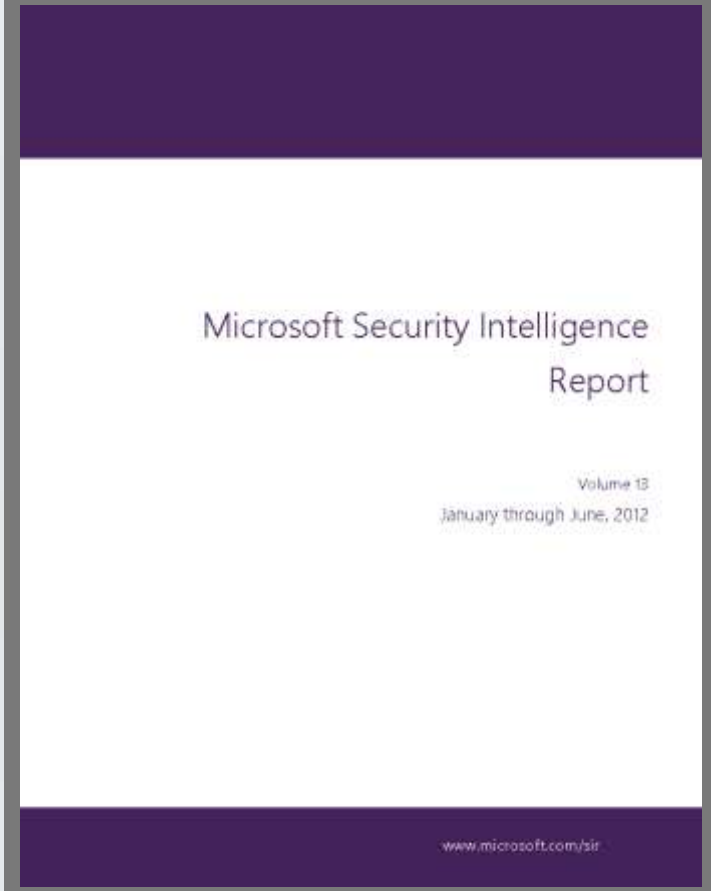
Malware / potentially unwanted software

SPAM, Phishing and drive-by attacks

Regional Threat Assessment

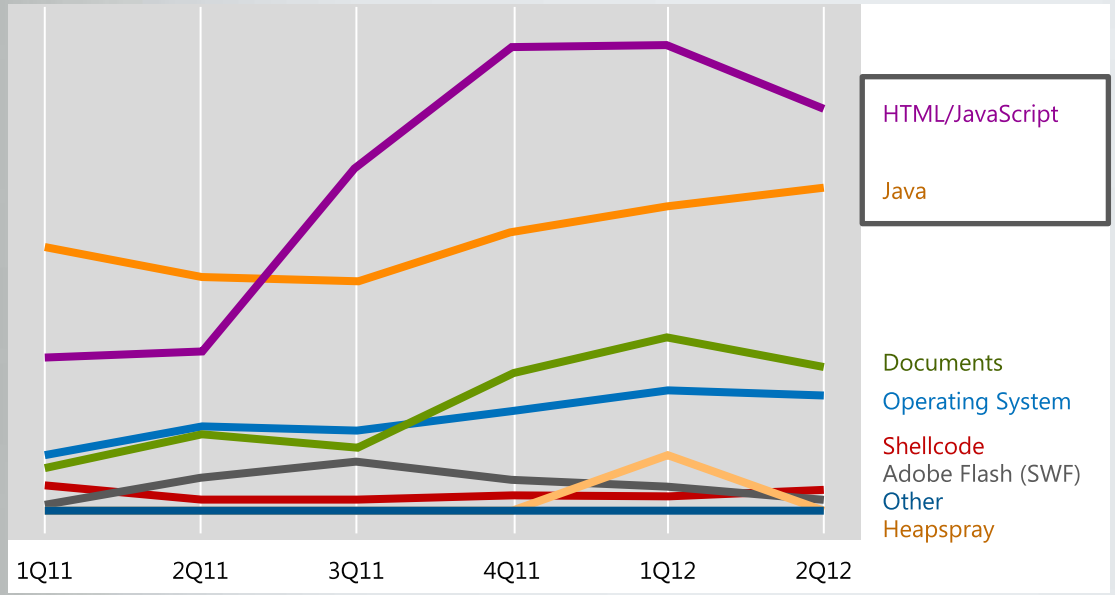
105 regions

www.microsoft.com/sir



Risk Indicators

Top Exploits



HTML/Java ➔ 70% of Top Exploit Families

Microsoft Security Intelligence Report

Volume 13
January through June, 2012

www.microsoft.com/sir

Free Tools to Manage Threats

Attack Surface Analyzer

- ✓ Baseline Analysis
- ✓ Incident Forensics

Anti-Cross Site Scripting Library

- ✓ Mitigate Cross Site Scripting Risks

Enhanced Mitigation Experience Toolkit

- ✓ Enable Mitigations
- ✓ Harden Legacy Apps

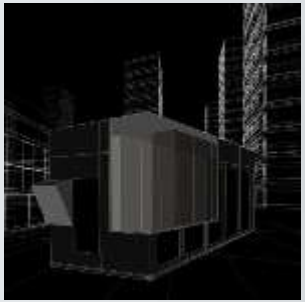
http://aka.ms/securitytools

Cloud Computing Study

Security – Perceived Barrier

Companies up to 500 PC's
ComScore independent study
No qualification by product or service
Five geographies

http://aka.ms/cloudstudy



Cloud Adoption *Benefits*

57%	3X	54%
Time Savings	Money Savings	Improved Security

Companies that realize the security benefits of the cloud…

…have more time, money to focus on their core business

Cloud Adoption *Barriers*

44%	61%	59%
Security Concerns	Industry Standards	Transparency

Companies citing security as a Cloud barrier …

… say standards and transparency would increase confidence

Removing Adoption Barriers

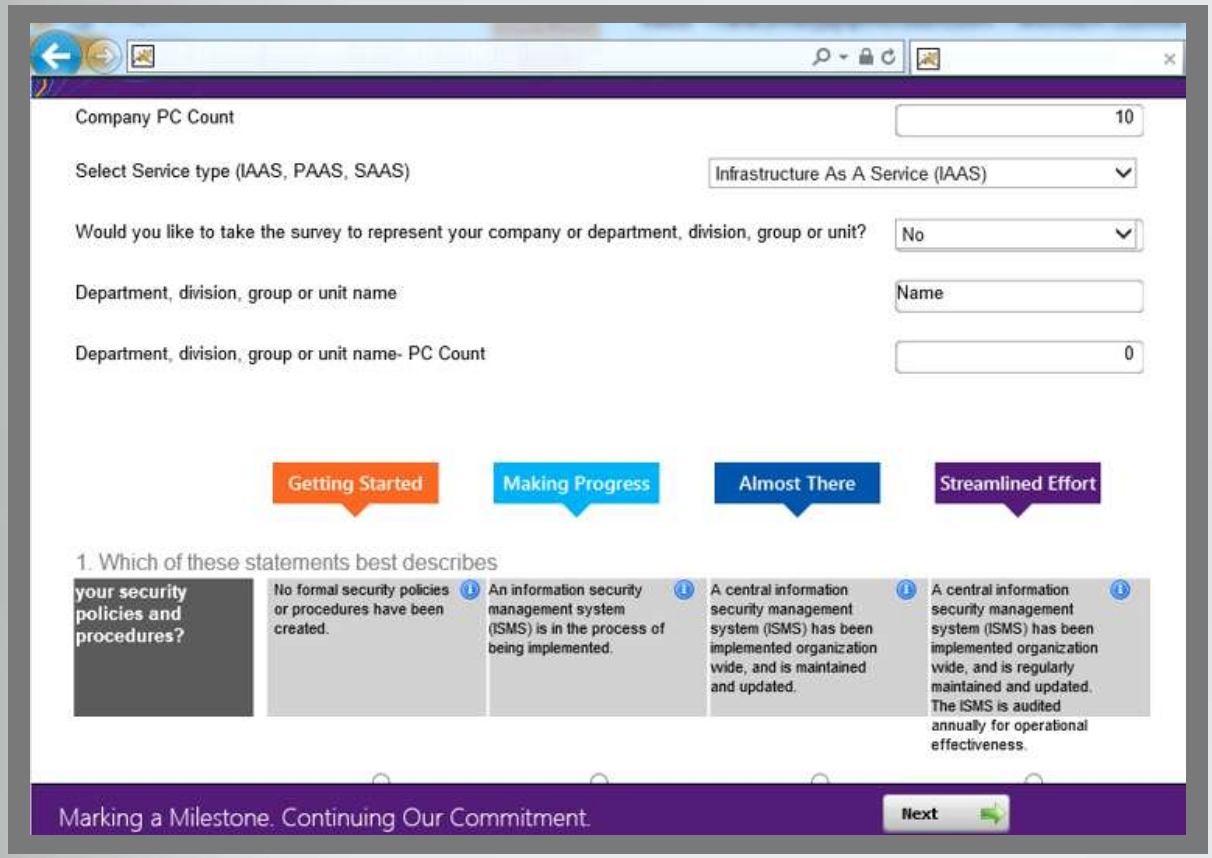
Collaborate to share information and guidance

Drive and support industry standards

Commit to transparency in cloud offerings

Cloud Security Readiness Tool

www.microsoft.com/trustedcloud



Where are we?

Where will we be?

Simplifies

Informs

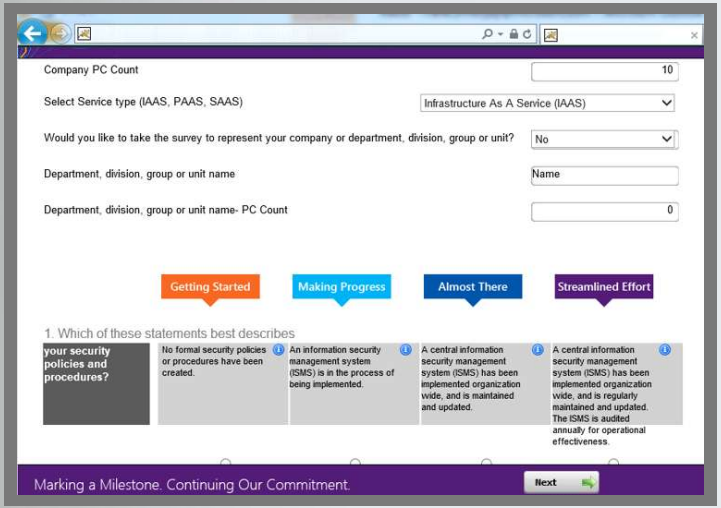
Enables

Agnostic

How it works

www.microsoft.com/trustedcloud

Online Survey



Cloud Security Control Areas:

cloud security alliance SM

- Security Architecture
- Legal
- Human Resources Security
- Risk Management
- Facility Security
- Release Management
- Information Security
- Resiliency
- Data Governance
- Operations Management

How it works

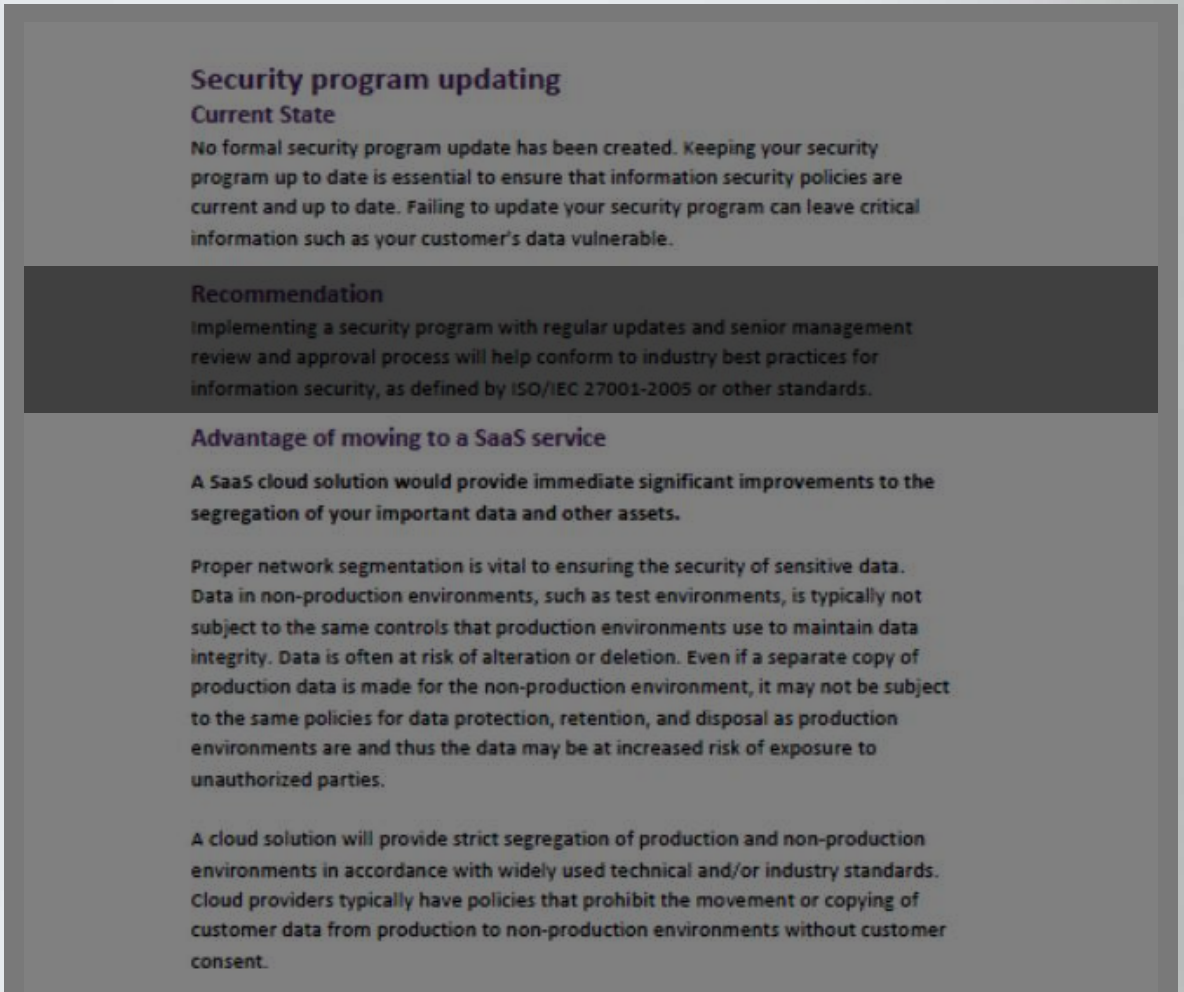
www.microsoft.com/trustedcloud

Online Survey

How it works

www.microsoft.com/trustedcloud

Generate Custom Report



Security program updating

Current State

No formal security program update has been created. Keeping your security program up to date is essential to ensure that information security policies are current and up to date. Failing to update your security program can leave critical information such as your customer's data vulnerable.

Recommendation

Implementing a security program with regular updates and senior management review and approval process will help conform to industry best practices for information security, as defined by ISO/IEC 27001-2005 or other standards.

Advantage of moving to a SaaS service

A SaaS cloud solution would provide immediate significant improvements to the segregation of your important data and other assets.

Proper network segmentation is vital to ensuring the security of sensitive data. Data in non-production environments, such as test environments, is typically not subject to the same controls that production environments use to maintain data integrity. Data is often at risk of alteration or deletion. Even if a separate copy of production data is made for the non-production environment, it may not be subject to the same policies for data protection, retention, and disposal as production environments are and thus the data may be at increased risk of exposure to unauthorized parties.

A cloud solution will provide strict segregation of production and non-production environments in accordance with widely used technical and/or industry standards. Cloud providers typically have policies that prohibit the movement or copying of customer data from production to non-production environments without customer consent.

How it works

www.microsoft.com/trustedcloud

Generate Custom Report

- ISO/IEC 27001-2005
- PCI DSS v2.0
- HIPAA / HITECH
- NIST SP800-53 R3

Regulation	Control details
HIPAA / HITECH Act	45 CFR 164.308(a)1(ii)(A) Risk analysis (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity. 45 CFR 164.308(a)8 Standard: Evaluation. Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.

Regulation	Control details
ISO/IEC 27001-2005	Clause 4.2.1 Establish the ISMS Clause 4.2.3 Monitor and Review the ISMS Clause 4.3.1 & 4.3.3 Control of Records A.7.2 Asset management A.15.1.1 Identification of applicable legislation A.15.1.3 Protection of organizational records A.15.1.4 Data protection and privacy of personal information

Regulation	Control details
PCI DSS v2.0	12.1 Establish, publish, maintain, and disseminate a security policy

Cloud Security Readiness Tool

www.microsoft.com/trustedcloud

Simplifies	Informs	Enables	Agnostic

Summary

Stay Informed

Embrace standards, best practices and transparency

Weigh the Risks and Rewards

adriennh@microsoft.com