End-To-End Computing

MAKING CYBER SIMPLE AND AFFORDABLE FOR YOU!!
Agenda

INTRODUCTION
INTRO TO CLOUD COMPUTING
CLOUD RESPONSIBILITIES
CLOUD SECURITY RISK
COMPLIANCE
DEMO (SECURING DATA & IDENTITIES)
Carlton Harris

Vice-President & Cofounder (Carlton Harris) has over 12 years of experience in information security and cybersecurity field supporting a vast number of government agencies such as; the US Navy, National Security Agency, US Army Intelligence command, and Department of State. Carlton’s technology proficiencies are in; SOC implementation, Incident Response and Cloud Security architect and design.

Esteve Mede

CEO & Cofounder (Esteve Mede) is a former Federal Chief Information Security Officer, with over 17 years of delivering results to both private and public sector. Esteve is a dynamic Information Technology Executive with a broad technology, Cyber security, operations and business background in diverse type of organizations. Adept at leading diverse, cross-functional and multinational teams. Highly skilled at merging disparate technologies and personnel into team-centered business units, leading to more efficient and creative solutions. Adept creating technology roadmaps, manage finances and deliver new functionality quickly and effectively. Talented team builder with knack for developing long range vision and translating it into reality.
Who We Are

A Virginia Small Business founded in 2012. Currently providing a broad spectrum of services and solutions in cybersecurity, software Development, and Big Data Analytics.

What we do

Cybersecurity & Information Assurance, Big Data Analytics, Project Management, DevOps

Company Vision

We help our customers by partnering with them to create solutions that meet their exact needs, then we apply the most efficient technologies and industry best practices to ensure that each customer achieve success in their businesses.
In the most simple form, cloud computing means storing, processing and accessing data and programs over the Internet instead of your computer's hard drive and Data Centers.
Cloud Service model

- **Software as a Service (SaaS)** - Capability for clients to use the provider’s applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser, or a program interface.

- **Platform as a Service (PaaS)** - Capability for clients to deploy their applications (created or acquired) onto the cloud infrastructure, using programming languages, libraries, services, and tools supported by the provider.

- **Infrastructure as a Service (IaaS)** - Capability for clients to utilize the provider’s processing, storage, networks, and other fundamental computing resources to deploy and run operating systems, applications, and other software on a cloud infrastructure.
Cloud Benefits:
- Efficiency & cost reduction
- Scalability
- Mobility
- Disaster recovery
- Security

The Cloud is having a measurable impact on business:

- 20.66% Average improvement in time to market
- 19.63% Average increase in company growth
- 18.80% Average increase in process efficiency
- 16.18% Average reduction in operational costs
- 15.07% Average reduction in IT spending
- 16.76% Average reduction in IT maintenance cost

Source: Varison Bower "The Business Impact of the Cloud"
Who is responsible

Control\Responsibility Matrix

<table>
<thead>
<tr>
<th></th>
<th>SaaS</th>
<th>PaaS</th>
<th>IaaS</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLIENT</td>
<td>Provides limited control over application configuration settings</td>
<td>Shifts the most Responsibility Hardware &amp; infrastructure to CSP but, Client maintains control over application configuration settings</td>
<td>Client maintains control over the OS, Storage networking.</td>
</tr>
<tr>
<td>CSP</td>
<td>Shifts the most Responsibility over to CSP but,</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Control \ Responsibility Example

Cloud Layer Example

<table>
<thead>
<tr>
<th>Service Model</th>
<th>IaaS</th>
<th>PaaS</th>
<th>SaaS</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIC &amp; communication infrastructure</td>
<td>CSP</td>
<td>CLIENT</td>
<td></td>
</tr>
<tr>
<td>Physical facilities</td>
<td>CSP</td>
<td>CLIENT</td>
<td></td>
</tr>
<tr>
<td>VMs</td>
<td>CSP</td>
<td>CLIENT</td>
<td></td>
</tr>
<tr>
<td>OS</td>
<td>CSP</td>
<td>CLIENT</td>
<td></td>
</tr>
<tr>
<td>Programming Languages</td>
<td>CSP</td>
<td>CLIENT</td>
<td></td>
</tr>
<tr>
<td>Applications</td>
<td>CSP</td>
<td>CLIENT</td>
<td></td>
</tr>
<tr>
<td>APIs, GUIs</td>
<td>CSP</td>
<td>CLIENT</td>
<td></td>
</tr>
<tr>
<td>Data</td>
<td>CSP</td>
<td>CLIENT</td>
<td></td>
</tr>
</tbody>
</table>

CSP CLIENT

Cloud Layer Example
How to start securing your environment

- International Standards Organization (ISO) 27K
- NZISM Protective Security Requirements (PSR) Framework
- Australien Signales Directorat (ASD) Essential 8
- Control Objectives for Information and Related Technology (COBIT)
- US National Institute of Standards and Technology (NIST)
- Industry-Specific Standards (HIPAA, PCI DSS, GDPR etc.)
This Framework consists of standards, guidelines, and best practices to manage cybersecurity-related risk. The Cybersecurity Framework’s prioritized, flexible, and cost-effective approach helps to promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security - NIST.
1. IDENTIFY
   - Identify and control who has access to your business information
   - Conduct background checks
   - Require individual user accounts for each employee
   - Create policies and procedures for cybersecurity

2. PROTECT
   - Limit employee access to data and information
   - Install Surge Protectors and Uninterruptible Power Supplies (UPS)
   - Patch your operating systems and applications routinely
   - Install and activate software and hardware firewalls on all your business networks
   - Secure your wireless access point and networks
   - Set up web and email filters
   - Use encryption for sensitive business information
   - Dispose of old computers and media safely
   - Train your employees

3. DETECT
   - Install and update anti-virus, anti-spyware, and other anti-malware programs
   - Maintain and monitor logs

4. RESPOND
   - Develop a plan for disasters and information security incidents

5. RECOVER
   - Make full backups of important business data and information
   - Continue to schedule incremental backups
   - Consider cyber insurance
   - Make improvements to processes/procedures/technologies
Applying Security to the modern enterprise
Secure Enterprise

**Identity**
Identity based security is a must as we shift the use of identities outside the perimeter.

**Apps and Data**
Identify and secure communications and data and application that align with business priorities.

**Infrastructure**
Protect current and new platforms with intelligence based security to detect and remediate vulnerabilities and attacks.

**Devices**
Ensure access to enterprise data is performed from trusted devices with hardware security assurances.
30/90 Day Action Plan

Rapid configuration:
- Basic admin protections
- Logging and audit configuration
- Enable identity based protections

Tenant configuration
Prepare stakeholders

Advanced protections:
- Admin accounts
- Data & user accounts
- Visibility into compliance, threat, and user needs

Adapt and implement default policies and protections

Adjust and refine key policies and controls
Extend protections to on-premises dependencies
Integrate with business and security processes (legal, insider threat, etc.)

Beyond
Improving your security posture

Recommendation
When you disable the automatic feature, it reduces your risk of data mishandling. When this setting is disabled, you won’t see the option in their email and existing user-created forwarding rules will no longer result in forwarded messages. If you still apply this setting, please ensure it is done with caution as it can impact your current process.

Security score
- Secure score: 704
- Recommendation: 7034 are ok

Resource health monitoring
- Critical: 47
- High: 5
- Medium: 3
- Low: 1

Instance Security Risk
- Active recommendations: 42

AWS Inspector - Findings
Inspector findings are potential security issues discovered during inspection’s assessment of the specified application. Learn more.
- Filters: ("/aws/aws/inspector:inspector;aws-apps/i0577506 is vulnerable to CVE-2020-4748") MyDemoApplication MyDemoAssessor
- Applications: MyDemoApplication MyDemoAssessor
- Findings: MyDemoApplication MyDemoAssessor

ServiceNow Security Center
- Review and improve your service level score and secure your service.
Securing your Cloud with Secure Score
# Reality Of Cloud Risk

## OWASP Cloud Top 10

<table>
<thead>
<tr>
<th>Rank</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Accountability &amp; Data Risk</td>
</tr>
<tr>
<td>2</td>
<td>User Identity Federation</td>
</tr>
<tr>
<td>3</td>
<td>Regulatory Compliance</td>
</tr>
<tr>
<td>4</td>
<td>Business Continuity &amp; Resiliency</td>
</tr>
<tr>
<td>5</td>
<td>User Privacy &amp; Secondary Usage of Data</td>
</tr>
<tr>
<td>6</td>
<td>Service &amp; Data Integration</td>
</tr>
<tr>
<td>7</td>
<td>Multi-tenancy &amp; Physical Security</td>
</tr>
<tr>
<td>8</td>
<td>Incidence Analysis &amp; Forensics</td>
</tr>
<tr>
<td>9</td>
<td>Infrastructure Security</td>
</tr>
<tr>
<td>10</td>
<td>Non-production Environment Exposure</td>
</tr>
</tbody>
</table>
store or process sensitive data in the cloud (e.g. financial records, business plans, source code, trading algorithms, etc.)

21% of organizations have experienced data theft from their cloud infrastructure.

- 16 million records exposed from hacking
- 404 million records exposed from unauthorized access
- 22 million records exposed from accidental exposure

27% have experienced data theft from their cloud infrastructure.
“Between January and August [2018], financial firms disclosed three times as many breaches as they did in the same period in 2016” - bitglass
Compliance and risk mitigation

Regulations are designed to ensure that organizations are protecting their customers’ financial information.

Payment Card Industry Data Security Standard (PCI DSS)
Sarbanes-Oxley Act (SOX)
Gramm-Leach-Bliley Act (GLBA)

They contain various requirements related to securing data access, responding to cyberattacks, and much more.

Failure to comply resulting in various fines

$100,000 per infraction under GLBA

$5+ million SOX

$500,000 per infraction PCI DSS
Reputation
Consequence
As companies move to the cloud to support employee mobility and easily scale to meet business needs, identities go beyond your boundaries and increase risk.

<table>
<thead>
<tr>
<th>Risk</th>
<th>Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password based attacks</td>
<td>Less privileged access</td>
</tr>
<tr>
<td>Brute force</td>
<td>Identity protection</td>
</tr>
<tr>
<td>Password spraying</td>
<td>Risk based alerting</td>
</tr>
<tr>
<td>Over privileged accounts</td>
<td>Multifactor Authentication</td>
</tr>
<tr>
<td>Multiple identities</td>
<td>Log collection</td>
</tr>
<tr>
<td>Lack of visibility</td>
<td></td>
</tr>
</tbody>
</table>
Identity Hardening & Alerting
As you find more value in data and more of it is produced, processed and stored in the cloud, your data also becomes a prime target for attackers that are looking to steal and resell data.

**Risk**
- Stolen information
- Reputation
- Loss of revenue
- Incurred penalties

**Control**
- Data Loss Prevention
- Secure Encryption
- Incident Response
- Strong pass phrases
- Really Secure Encryption
Protecting Cloud-Deployed Data
End-To-End Computing
Email: INFO@EECOMPUTING.COM
Website: www.eecomputing.com
Phone: 833.720.7770

@EndtoEndComp
@end-to-end-computing-llc
References

- https://www.eecomputing.com/blog/design-a-stunning-blog
- https://www.owasp.org/index.php/Category:OWASP_Cloud_%E2%80%90_10_Project
- https://www.idtheftcenter.org/breachclarity/