CLOUDY WITH A CHANCE OF DIGITISATION

SCOTT MANSON
MANAGING DIRECTOR-MIDDLE EAST & TURKEY

www.menaisc.com
Eradicating the fantasy of a Magic Silver bullet past 112 years.
PHILOSOPHY:
AGGREGATION OF MARGINAL GAINS
VERSUS
IMPROVING EVERYTHING BY
BEING UNBEATABLE SOMEDAY

1-2%

...
Focus on being a little safer everyday

Versus

Being perfectly unhackable someday

...
What is stopping us going faster?
• To Clouds
• From Clouds
• Between Clouds
STRIKE THE CLOUD BALANCE

DATA SOVEREIGNTY

CONTROL

SPEED AND SCALE

ECONOMICS AND VALUE
The Kingdom of Saudi Arabia’s NCA published the Essential Cybersecurity Controls in 2018.
The National Cybersecurity Authority established the Essential Cybersecurity Controls (ECC 2018: 1)

**Consists of:**
- 5 Main Domains for Cybersecurity Controls
- 29 Subdomains for Cybersecurity Controls
- 114 Cybersecurity Controls

**Applies to**
- Government entities in the Kingdom of Saudi Arabia (including ministries, agencies, institutions, etc.),
- Government affiliates
- Private sector entities that have or operate or host national critical infrastructures (CNI)
Mapping ECC To Cloud Computing

- Domain 4 Specifically Covers Cloud Computing

- You Need Control of Data
  - **To** Clouds
  - **From** Clouds
  - **Between** Clouds
  - Cloud Configuration

- Cloud Security Is A Shared Responsibility
Cloud 3600 Shared Responsibility Model

© McAfee 2019. OK for reuse if unedited
Example: Identity & Access Management

• Check all cloud applications
• Communicate to all owners
  • Are they integrated with SSO?

*User Responsibility*

*Enterprise Responsibility*

*Service Provider feature, enterprise configuration*

*Service Provider Responsibility*

© McAfee 2019. OK for reuse if unedited
# How To Map ECC To Cloud Computing

<table>
<thead>
<tr>
<th>Control</th>
<th>ECC Text (shortened)</th>
<th>Cloud Controls Required</th>
<th>MVISION Cloud Capabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-5-3-3</td>
<td>Risk assessment must be implemented during the planning phases of obtaining third-party services.</td>
<td>Cloud use may bring in risk, this should be assessed before use and visibility into shadow cloud service use and risk reviewed.</td>
<td>The cloud registry of &gt;20,000 services contains &gt;70 constantly updated attributes to ascertain risk.</td>
</tr>
<tr>
<td>2-4-2</td>
<td>Email service protection must be implemented.</td>
<td>Cloud-based email services must be controlled.</td>
<td>Cloud-based email (such as Exchange online) can be monitored and controlled.</td>
</tr>
<tr>
<td>2-5-3-3</td>
<td>Network security management must include restrictions on the use of file storage/sharing.</td>
<td>Cloud storage, sharing, and through-cloud collaboration must be controlled.</td>
<td>A wide set of controls are available to control access, upload, download, sharing, and collaboration are available for many cloud services/devices/location/users.</td>
</tr>
<tr>
<td>4-2-3-1</td>
<td>Data must be classified prior to hosting on a cloud service.</td>
<td>Cloud services must accept prior classifications of data.</td>
<td>If data is not classified, MVISION Cloud can add classification or stop data being uploaded to cloud services.</td>
</tr>
</tbody>
</table>
Mapping ECC To Cloud Computing: Paper Available
<table>
<thead>
<tr>
<th>Technology</th>
<th>IaaS</th>
<th>PaaS</th>
<th>SaaS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link control, domain check, email controls, encryption</td>
<td><img src="#" alt="Green" /></td>
<td><img src="#" alt="Green" /></td>
<td><img src="#" alt="Green" /></td>
</tr>
<tr>
<td>User Behavior analytics, user &amp; device policies</td>
<td><img src="#" alt="Green" /></td>
<td><img src="#" alt="Green" /></td>
<td><img src="#" alt="Green" /></td>
</tr>
<tr>
<td>DLP, on demand scan</td>
<td><img src="#" alt="Green" /></td>
<td><img src="#" alt="Green" /></td>
<td><img src="#" alt="Green" /></td>
</tr>
<tr>
<td>Compromised account detection, malware scanning</td>
<td><img src="#" alt="Green" /></td>
<td><img src="#" alt="Green" /></td>
<td><img src="#" alt="Green" /></td>
</tr>
<tr>
<td>SSO integration</td>
<td><img src="#" alt="Green" /></td>
<td><img src="#" alt="Green" /></td>
<td><img src="#" alt="Green" /></td>
</tr>
<tr>
<td>Configuration audit</td>
<td><img src="#" alt="Green" /></td>
<td><img src="#" alt="Green" /></td>
<td><img src="#" alt="Green" /></td>
</tr>
<tr>
<td>Audit of cloud configurations</td>
<td><img src="#" alt="Gray" /></td>
<td><img src="#" alt="Gray" /></td>
<td><img src="#" alt="Gray" /></td>
</tr>
<tr>
<td>CIS benchmarking</td>
<td><img src="#" alt="Gray" /></td>
<td><img src="#" alt="Gray" /></td>
<td><img src="#" alt="Gray" /></td>
</tr>
<tr>
<td><strong>Collaboration</strong> control</td>
<td><img src="#" alt="Blue" /></td>
<td><img src="#" alt="Blue" /></td>
<td><img src="#" alt="Blue" /></td>
</tr>
<tr>
<td><strong>User/Device/Data</strong> control</td>
<td><img src="#" alt="Blue" /></td>
<td><img src="#" alt="Blue" /></td>
<td><img src="#" alt="Blue" /></td>
</tr>
<tr>
<td><strong>Data</strong> Classification &amp; Accountability</td>
<td><img src="#" alt="Blue" /></td>
<td><img src="#" alt="Blue" /></td>
<td><img src="#" alt="Blue" /></td>
</tr>
<tr>
<td><strong>End-Point</strong> Protection</td>
<td><img src="#" alt="Blue" /></td>
<td><img src="#" alt="Blue" /></td>
<td><img src="#" alt="Blue" /></td>
</tr>
<tr>
<td><strong>Identity</strong> &amp; Access Management</td>
<td><img src="#" alt="Blue" /></td>
<td><img src="#" alt="Blue" /></td>
<td><img src="#" alt="Blue" /></td>
</tr>
<tr>
<td><strong>Application</strong> Level Controls</td>
<td><img src="#" alt="Blue" /></td>
<td><img src="#" alt="Blue" /></td>
<td><img src="#" alt="Blue" /></td>
</tr>
<tr>
<td><strong>Network</strong> Control</td>
<td><img src="#" alt="Gray" /></td>
<td><img src="#" alt="Gray" /></td>
<td><img src="#" alt="Gray" /></td>
</tr>
<tr>
<td><strong>Host</strong> Infrastructure</td>
<td><img src="#" alt="Gray" /></td>
<td><img src="#" alt="Gray" /></td>
<td><img src="#" alt="Gray" /></td>
</tr>
<tr>
<td><strong>Physical Security</strong></td>
<td><img src="#" alt="Gray" /></td>
<td><img src="#" alt="Gray" /></td>
<td><img src="#" alt="Gray" /></td>
</tr>
</tbody>
</table>

© McAfee 2019. OK for reuse if unedited
Approaching NCA ECC Compliance

Timeline

- Initial Assessment
- Implement Critical Security Controls
- Formalize Security Organization
- Develop Governance Framework

Short to Long term Initiatives

- Develop Cyber Risk Management Framework
- Risk Based Control Deployment
- Develop Standards and Guidelines
- Embed Review and Improvement Cycle
McAfee technologies’ features and benefits depend on system configuration and may require enabled hardware, software, or service activation. Learn more at mcafee.com. No computer system can be absolutely secure.

This document contains information on products, services and/or processes in development. All information provided here is subject to change without notice at McAfee’s sole discretion. Contact your McAfee representative to obtain the latest forecast, schedule, specifications, and roadmaps.

McAfee, the McAfee logo, ePolicy Orchestrator, and McAfee ePO are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the U.S. and/or other countries. Other names and brands may be claimed as the property of others. Copyright © 2018 McAfee, LLC.