## Operational Maturity: Security Risk Rating

### Level 1: High Risk
- Not all devices using endpoint protection
- Using standard spam filter
- No 2FA Policy
- Not using firewalls at every site
- Not being monitored by SOC
- No image based backups
- Not doing patch management
- No cybersecurity training for employees
- No password policies
- No tools in use, common PWs used across apps/sites

### Level 2: Medium Risk
- All devices have AV but using legacy, signature based protection
- Some use of advanced spam filter
- Some apps using 2FA and SSO
- Advanced firewalls but no IDS system
- Network monitoring OR log monitoring from a SOC, but not both
- Semi-regular image based backups of critical data
- Only doing patch management for some servers
- Annual cybersecurity training for all employees
- Some apps using robust password policy
- Some unique PWs used, not organized or centralized

### Level 3: Lower Risk
- All devices have a next-gen endpoint protection that can detect file-less attacks
- Using advanced email protection
- Most apps using 2FA and SSO
- Advanced firewall and IDS
- Full network and log monitoring by SOC
- Regular image based backups of all critical data
- Fully enrolled in patch management
- Monthly cybersecurity training for all employees
- All apps using robust password policy
- All Passwords stored, organized and unique across all apps

### Current Risk Rating

<table>
<thead>
<tr>
<th>Endpoint / AV</th>
<th>Email Protection</th>
<th>2FA / SSO</th>
<th>Firewall / IDS</th>
<th>Security Monitoring</th>
<th>Backup</th>
<th>Patch Management</th>
<th>Training</th>
<th>Password Policy</th>
<th>Password Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not all devices using endpoint protection</td>
<td>Using standard spam filter</td>
<td>No 2FA Policy</td>
<td>Not using firewalls at every site</td>
<td>Not being monitored by SOC</td>
<td>No image based backups</td>
<td>Not doing patch management</td>
<td>No cybersecurity training for employees</td>
<td>No password policies</td>
<td>No tools in use, common PWs used across apps/sites</td>
</tr>
<tr>
<td>All devices have AV but using legacy, signature based protection</td>
<td>Some use of advanced spam filter</td>
<td>Some apps using 2FA and SSO</td>
<td>Advanced firewalls but no IDS system</td>
<td>Network monitoring OR log monitoring from a SOC, but not both</td>
<td>Semi-regular image based backups of critical data</td>
<td>Only doing patch management for some servers</td>
<td>Annual cybersecurity training for all employees</td>
<td>Some apps using robust password policy</td>
<td>Some unique PWs used, not organized or centralized</td>
</tr>
<tr>
<td>All devices have a next-gen endpoint protection that can detect file-less attacks</td>
<td>Using advanced email protection</td>
<td>Most apps using 2FA and SSO</td>
<td>Advanced firewall and IDS</td>
<td>Full network and log monitoring by SOC</td>
<td>Regular image based backups of all critical data</td>
<td>Fully enrolled in patch management</td>
<td>Monthly cybersecurity training for all employees</td>
<td>All apps using robust password policy</td>
<td>All Passwords stored, organized and unique across all apps</td>
</tr>
</tbody>
</table>

## Ready To Learn More?
(855) PPL.GUYS | PurpleGuys.com