Enterprise Security Initiative Roadmap

Sunil Rachakonda
As of September 18, 2018
Two-Step Verification
<table>
<thead>
<tr>
<th>Product - Action Required</th>
<th>Deadline</th>
<th>Who May Be Affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Two-Step Verification – ensure email address is valid</td>
<td>10/10/2018</td>
<td>Single Sign-On Tool Users (slide 10)</td>
</tr>
<tr>
<td>Two-Step Verification – Review FAQ document</td>
<td>10/10/2018</td>
<td>Single Sign-On Tool Users (slide 10)</td>
</tr>
</tbody>
</table>
### 2018 Roadmap for Enterprise Security

<table>
<thead>
<tr>
<th></th>
<th>Apr</th>
<th>May</th>
<th>Jun</th>
<th>Jul</th>
<th>Aug</th>
<th>Sep</th>
<th>Oct</th>
<th>Nov</th>
<th>Dec</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Screen resolution identification</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Train:</strong> August 8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Production: September 12</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Two-Step Verification</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Train:</strong> August 15</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Production: October 10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

[www.pjm.com](http://www.pjm.com)
What Does Two-Step Verification Provide?

- Provides an extra layer of security to PJM’s single sign on tools
- Uses a password and additional information – a token
  - Used by banks, government sites and some email providers
- Prevents a breach even if a password is successfully compromised
- Already in use with PJM’s Account Manager application
How Does Two-Step Verification Work?

- Triggered on logon from an unrecognized device
- Uses a password and email token combination
- Validated email addresses become essential
- CAMs will be able to manage email domains (e.g., @pjm.com)
- Leverages valid email addresses
- PJM will provide a means to manage email domains
Three Easy Steps

1. Sign in

2. PJM Account Manager Soft Token
   - Account Manager_STG <accountmanager-donotreply@pjm.com>
   - Sent: Mon 10/16/2017 12:08 PM
   - To: [Redacted]
   - Hello [Redacted]
   - You have requested a Soft Token for [Redacted]
   - Your Soft Token is 08188826
   - Please return to your browser and enter this token into the form to finish your login.
   - Note that this Soft Token will expire in 10 minutes.

3. Enter Soft Token
   - Finish Login
   - Sign Out
Ease of Use

Single User Multi Account (SUMA)
- Reduces the number of accounts

Works with mobile devices

Allows up to five unique devices per user
- Browsers
- Laptops/computers

Screen resolution
- No longer a factor in device identification

Clearing browser cache
- Will not remove the device
Only Browser-based Interactions

• No Browserless/API impacts at this time
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Non Impacted Applications</td>
<td>PJM.com, eDART, eGADS</td>
</tr>
<tr>
<td>Area</td>
<td>Impact</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>Browserless (XML API)</td>
<td>None</td>
</tr>
<tr>
<td>Browser</td>
<td>One time password requirement with each new device</td>
</tr>
</tbody>
</table>
• There is an FAQ document on PJM.com
Appendix - Enterprise Security
Security Drivers

PJM’s priority is to protect the accounts, data and information entrusted by our members.

Critical infrastructure is a higher profile target:

- Nation states are increasing their attacks.
- Password spraying has become an effective tool to compromise user accounts.

PJM recognizes member feedback must be incorporated into security approaches.
PJM’s Response to Cyber Threats

More restrictive cybersecurity controls

Block network traffic from outside the U.S. and Canada via Geo-IP blocking
PJM’s Approach to Geo-IP Blocking

- Analyze network traffic by country
- Analyze the use of authenticated services by authorized user
- Correlate service use against analysis of traffic by country
- Build up whitelisting for valid, correlated network traffic
- Monitor whitelisting
- Successively block groups of countries based on risk/use
PJM’s Support/Response Approach

Communicate change process

Collecting the right feedback to quickly determine username, source IPs, services being accessed, error information, etc.

Response process for member-related problems

An escalation process in place to quickly respond to problems

Regular meetings to review process effectiveness
What Has PJM Done to Date?

PJM has begun implementing Geo-IP blocking with:

- High risk countries
- Limited access to internet SCADA