Enterprise Security Initiative Roadmap

Colin Brisson
Manager, Enterprise Information Security
As of June, 2018
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
- Response process for member-related problems
- Regular meetings to review process effectiveness

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

An escalation process in place to quickly respond to problems
PJM has begun implementing Geo-IP blocking with:

- High risk countries
- Limited access to internet SCADA
Two-Step Verification

Foluso Afelumo
Manager, Development and Data Operations
As of June, 2018
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
   - Username:
   - Password:
   - Sign In
   - Forgot Password
   - Register

2. PJM Account Manager Soft Token
   - Account Manager_STG <accountmanager-donotreplay@pjm.com>
   - Sent: Mon 10/16/2017 12:08 PM
   - To: 
   - Hello 
   - You have requested a Soft Token for 
   - 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
   - Request New Soft Token

NOTICE: This system and the information processed or contained within is for the use of authorized users only. Any use, and for any lawful purpose, PJM may monitor, intercept, record and search any communications or data transiting or stored on this information system, and may disclose such communications or data to the U.S. Government and its authorized representatives. Anyone using this system expressly consents to the terms and conditions contained in this notice. Individuals using this computer system without authority, or in excess of their authority, are advised that if monitoring reveals possible improper or criminal activity, system personnel may provide the evidence of such monitoring to management or law enforcement officials for disciplinary proceedings and/or criminal and civil proceedings under local and foreign laws.
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
Scope

Only Browser-based Interactions

• No Browserless/API impacts at this time
### Scope

<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>
May 31
SUMA available for all applications (except eCredit, MSRS and Oasis in training environment)

Late June
SUMA available for all applications (except eCredit, MSRS and Oasis in production environment)

August 10
Participants consolidate subaccount user accounts into SUMA accounts in the training environment

August 15
Two-step verification goes live in training

August 31
Email verification feature available in training environment

September 10
Two-step verification goes live in the production environment for PJM employees

September 30
- Participants consolidate sub-account user accounts into appropriate SUMA accounts
- Email verification feature available in production environment

October 10
Two-step verification goes live in the production environment for stakeholders
## 2018 Roadmap for Enterprise Security

<table>
<thead>
<tr>
<th>April</th>
<th>May</th>
<th>June</th>
<th>July</th>
<th>August</th>
<th>September</th>
<th>October</th>
<th>November</th>
<th>December</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Train:</strong> August 15</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><strong>Production:</strong> October 10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

**Tech Change Community**

[www.pjm.com](http://www.pjm.com)