**January 2016 WGM - Meeting Minutes**

<table>
<thead>
<tr>
<th>Date: 2016/01/12</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time: Tuesday Q2</td>
</tr>
</tbody>
</table>

**Called by**: HL7 Electronic Services and Tools WG

**Facilitator**: Andy Stechishin

**Purpose**: WGM

**Note taker(s)**: David Burgess

**Attendees**: Andy Stechishin, Alexander Henket, Johnathan Coleman, Jeff Brown, Ken McCaslin, Mark McDougall, Charles Jaffe, Nat Wong, David Burgess, Dave Hamill

**Regrets**:

**Agenda Topics**

*Update and wiki.hl7.org incident*

*Establish day and time for regular scheduled calls*

**Minutes/Conclusions Reached:**

**Update and wiki.hl7.org incident:**

- Dave, Ken, and Mark gave the EST group an overview of what happened:
  - Wednesday Tamara identified several accounts that appeared to be created by bot accounts and deleted them. She later found over 150 bogus accounts. At that time she stopped the ability to auto add accounts. Research discovered over 10,000 bogus pages had been created.
  - When attempting to recover from backup it was discovered that the backup was a two-step process. Step one back up the wiki database, step two copy backup file to backup media. Step two had been working correctly, however the first step was failing do to it being tied to a user account that was no longer valid.
- Ken introduced us to Johnathan Coleman from Security Risk Solutions, Inc. who volunteered his organization to help us investigate the incident, and to provide recommendations on how to prevent future risk.
- Various items in regards to the issue where discussed including:
  - 2 factor authentication
  - Regular testing of the backups
  - Issues with using common user naming conventions
  - Disabling account with no activity for over 30 days, or forcing a password reset
  - Possibility of using “OAuth”
  - Change system activities away from “user” accounts to “roll-based” account.
  - Authenticating new wiki accounts
  - Conducting users audits
- After general discussion we stopped and broke down the discussion into:
  - What is the pain point:
    - What are the steps moving forward? A set plan for different Incidence Response Plans depending on type of attack.
    - What do we do now, how we close that out.
    - Get successful backup in place, and test the ability to restore.
    - Backup with a roll based account, instead of user account. (We were informed that this has already been put into place.)
    - Don Lloyd restored all links on main wiki except 6, reaching out to manager of those six areas.
    - Presently 2000 orphaned pages
    - Motion to have Johnathan’s team look at server, and into the incident.
      - **Motion by Ken, seconded by Nat passed unanimously**
  - Craft Message to be released to HL7 community.
    - Group agreed to have Ken craft a message to release to the HL7 community (announcement at general session). Message in general to state: Issue has been identified, we are treating seriously, external expert engaged to review and advice. Steps are being taken to prevent this going forward. During review process new accounts are still locked. Newly identified issues should be reported to webmaster.
**Establish day and time for regular scheduled calls:**

- Going forward we will schedule meetings on Tuesday at 3:00pm EST, with the first meeting next week, to stay engaged with status of wiki incident.