Notes from the UW System CIO Council Video Conference

May 17, 2012

Agenda

Research and Education Network Update

TISC - Software Demonstration

TISC - Two-Factor Authentication

Voyager/IAM Shibboleth Project Update

Central Hosting of WordPress

MOR Leadership Program
D2L Upgrade
Next Meeting

Attendees

<table>
<thead>
<tr>
<th>CIOs and their Representatives</th>
<th>Guests</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nancy Crabb</td>
<td>Mark Clements</td>
</tr>
<tr>
<td>David Dumke</td>
<td>Lorie Docken</td>
</tr>
<tr>
<td>Nick Dvoracek</td>
<td>Dan Frommelt</td>
</tr>
<tr>
<td>Chip Eckardt</td>
<td>Ty Letto</td>
</tr>
<tr>
<td>Mohamed Elhindi</td>
<td>Chris Liechty</td>
</tr>
<tr>
<td>Paula Ganyard</td>
<td>Mitch Lundquist</td>
</tr>
<tr>
<td>Lee Goldesberry</td>
<td>Paul Moriarty</td>
</tr>
<tr>
<td>Marcia Henfer</td>
<td>Jim Treu</td>
</tr>
<tr>
<td>Tom Jahnke</td>
<td>Peter Zuge</td>
</tr>
</tbody>
</table>
Research and Education Network Update

Ed Meachen and David Lois reminded the CIO Council that new Wisconsin statutes require the UW System (UWS) to leave WiscNet and its Board of Directors. Given this state of affairs, the goals of WiscNet and the UWS are to preserve the value and resources of WiscNet for its current membership and to preserve and enhance the research and education networking capabilities of the UWS. These resources and capabilities have been built up over the last 20 years.

TISC - Software Demonstration

Representing the Technology & Information Security Council (TISC), Peter Zuge introduced five-minute software demonstrations for:

- Securing the Human
- Securing the Data
- Securing the Machine

Jim Treu demonstrated the SANS Securing the Human security awareness training resources, which are nicely packaged with PDF newsletters for subject matter training; email and print versions of posters; a customizable screen saver; and SCORM modules that can be imported into learning management systems (LMS) such as D2L. Institutions could use the built-in SCORM modules for reporting module, or create their own.

Mark Clements and Peter Zuge demonstrated the use of IdentityFinder for securing the data. It is a client server application for Windows or Mac that employs centrally managed policies to scan for personally identifiable information or other sensitive data on personal workstations. Information is sent back to a central repository for reporting and display on a dashboard. The software can be set up to automatically take action on discovered data, such as implementing quarantine procedures. One challenge is that there is no fool-proof way to secure data on a personal workstation because attack
vectors and vulnerabilities are continually shifting. For now, it is important to at least know where sensitive data resides and to consider whether it can be deleted or moved to some place more secure. A four-person implementation team is starting to work through the workstations at UW-Oshkosh, beginning with the functional areas. The UWS institutions that don’t already have a process in place are encouraged to consider using IdentityFinder.

Peter Zuge demonstrated the use of Secunia CSI for securing the machine. It scans PC workstations to identify vulnerable software in both the operating system and the applications. Scans can be conducted via a local agent on the workstation that doesn’t require administrative rights. A central management console can report all the vulnerable software present on a given workstation. Secunia is a good tool for verifying the data that comes from SCCM because it uses a different API call and scans the applications directly. Version 5 will also work with Macs.

**TISC - Two-Factor Authentication**

Chris Liechty explained the challenges in coming to system-wide consensus on two-factor authentication. The official report will come out in a couple weeks. Use of both smart cards and USB tokens in concert with the UW Digital ID are the options that will receive full support. There will also be a Flexible Option for institutions that choose to use Shibboleth with a different hardware token. The token will need to be reviewed by TISC and a newly forming IAM Technical Advisory Group and approved by the IAM Steering Committee. The Flexible Option would also require the institution run its own Identity Provider. The Flexible Option would allow iOS devices to be used with one-time passwords and RSA tokens. If the CIOs support the Flexible Option as it is outlined in the report, they will need to push for the resources to support it.

Elena Pokot discussed the tradeoffs in whether the Flexible Option would replace an existing project or receive additional funding. She has talked with the new Director of the UWS Service Center regarding HRS and learned that they are also in the design stage with respect to two-factor authentication. The IAM, middleware and HRS projects need to stay aligned.

**Voyager/IAM Shibboleth Project Update**

Ty Letto and Mitch Lundquist reported that the DoIT Middleware Services and the University of Wisconsin Libraries have partnered for a couple years on authentication strategies for the Voyager Forward application. Voyager IDs are a little different at each UWS institution. Wisconsin Federation, SAML 2.0 and Shibboleth are the replacement option for the retirement of the IAA Authorization Hub later this year. This will require that Voyager IDs be delivered directly from the institutional directories to the Identity Provider. Such a strategy does not rule out an institution choosing to be its own Identity Provider down the line. It also sets the stage for expanding the Wisconsin Federation beyond the UW System to other K-12 and post-secondary institutions.
The campus configurations for several UWS institutions are complete and their Voyager IDs are being passed to the Forward application. The team is working with the remaining institutions through the contacts named on the IAA support list. Mohamed Elhindi recommended that the CIO Council be copied on communications that involve policy and technical decisions.

In the future, the Voyager IDs will facilitate system-wide interlibrary loan and a new resource discovery tool that will be chosen soon.

**Central Hosting of WordPress**

Chip Eckardt explained that UW-Eau Claire faculty are creating content with WordPress and displaying it within D2L. He suggested that better integration would allow use of the same username and password for both systems. WordPress is in use at many of the UWS institutions for academic and/or administrative purposes, but none are integrating it with D2L in the same fashion.

It was recommended Learn@UW Executive Committee look at this issue because there are pressures to couple many products with D2L. Elena Pokot noted the emerging Learning Tools Interoperability (LTI) standard as one of many approaches for integrating products and authentication with Learning Management Systems. The IAM Executive Committee and the Learn@UW Executive Committee should move carefully given the many emerging standards and the new functionalities that will be included in the next release of D2L.

Nick Dvoracek noted that one advantage to using a tool like WordPress in addition to D2L is that it allows faculty to create content that can be distributed both to the general public as well as to students.

**FY13 MOR Leadership Program**

Ed Meachen reported that a couple members of the current MOR Leaders Program will give a presentation at the UWS CBO retreat in June. Both CIOs and CBOs may be interested in sending selected staff to the program in FY13 that Lorie Docken will coordinate. CIOs should send a count of the number of potential IT participants from their institutions to Ed Meachen by the end of June. All of the CIOs are invited to the graduation of the participants in the current program at UW-Stevens Point on June 27th.

**D2L Upgrade**

The Learn@UW site admins have been briefed about the upgrades and outages to D2L that are planned for the end of June.

**Next Meeting**

The next CIO Council meeting will be on June 21 at 780 Regent Street in Madison. Future meeting dates, the directory of UWS CIOs, and CIO