**Information Security Review**

In 2013, the Information Security Office and IT leadership began discussions about the information security technology and processes in the data center. Collaboratively, these stakeholders through a competitive bid process commissioned Presidio, Inc. to perform a data center security review to provide a strategy to improve the security posture. This request was predicated on the concept of an IT network “architectural” review that was recommended in 2011 as part of a plan to develop the Information Security function in conjunction with the upgrade of the physical infrastructure of the data centers in Orono and Portland. Upon completion of the data center project and the establishment of a core Information Security foundation, the next step was to examine the data center information security.

Presidio completed its data center review in December 2013. Their report included 27 findings and recommendations which they grouped in five areas of risk: Configuration Management, Account Management, Data Center On-Boarding, Secure Network Engineering and Boundary Controls, and Centralized Log Management. Some of these recommendations are primarily process oriented while others require investment in technology solutions such as firewalls.

To address the findings and recommendations, a team of IT and Information Security staff have developed a three-year plan of action for the issues presented. This UMS response includes nine separate initiatives. These initiatives are lined up over three years based on potential funding availability, ability to execute, and dependencies that the initiatives have on one another. Some of the initiatives require a substantial time investment to evaluate alternative solutions, to conduct a competitive procurement process, or to implement. The cost of the recommendations includes initial, one-time costs for equipment, $670K, and recurring maintenance, $162k. Because these new functions require configuring, managing and maintaining new equipment it is estimated three new FTE positions in infrastructure and operations would be required. The estimated annual salary and benefits for these new positions is $270k.

Although Presidio recommends future actions for the data centers beyond the core findings and recommendations, it is likely that the result of these nine initiatives will prove that the data centers are reasonably secure. However, the scope of this activity was limited and following these actions, the UMS should focus attention on other parts of the IT infrastructure. Additionally the dangers to information security continue to evolve as do compliance requirements, so the UMS will need to conduct periodic reviews and make future investments to remain secure.
INFORMATION SECURITY REVIEW

Findings and Response
Overview - Scope of Review

- In 2013, a project was initiated to:
  - Review information security processes and procedures of systems, storage, and networks located in UMS data centers
  - Provide strategic recommendations for improved secure service delivery

- Presidio performed the review and issued a report in December 2013
  - 27 unique findings/recommendations
Background: Data Center Facilities Project

• In July 2007 - 2011 facilities consultants identified:
  • Physical deficiencies
  • Mechanical deficiencies
  • Electrical system deficiencies

• The facilities project included:
  • Hardening the physical environment
  • New HVAC and fire suppression systems
  • New power distribution and backup generator
Background: Data Center Facilities Project

- The project did not cover:
  - Consolidation of campus/department resources
  - System or Network Security

- The project preceded:
  - Formation of the Office of Information Security
Background: Information Security Start-up

• 2011 Plan, Funding and Accomplishments:
  • Executive leadership at the UMS level
  • Collaborative updating of policy and standards
  • System-wide user education
  • Vulnerability scans
  • Enhanced central monitoring and response
  • Centralized IT assets at the campus level
Background: Information Security Start-up

- The original plan stated…
  
  “Re-architect general security infrastructure coincident with IT centralization”

- Details included:
  - Server architecture review
  - Improved segmentation/isolation
Presidio Summary – Areas of Risk

- Configuration Management
  - Too many independent IT groups all with their own processes and procedures

- Account Management

- Data Center On-Boarding
  - Standards for bringing new systems into the data centers

- Secure Network Engineering & Boundary Controls
  - Differing security zones based on use of systems

- Centralized Log Management
<table>
<thead>
<tr>
<th>Initiative</th>
<th>Description</th>
<th>Cost</th>
<th>Fiscal Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>End-User VPN Remote Access</td>
<td></td>
<td>$40K</td>
<td>FY14</td>
</tr>
<tr>
<td>Web Proxy Server</td>
<td>Supports software updates/patches</td>
<td>$10K</td>
<td>FY14</td>
</tr>
<tr>
<td>Management Fire-wall &amp; VPN</td>
<td>Separates management access from end-user access</td>
<td>$10K</td>
<td>FY15</td>
</tr>
<tr>
<td>Configuration Management Tools</td>
<td>Tools to standardize, maintain, and audit configuration of systems</td>
<td>$50K</td>
<td>FY15</td>
</tr>
<tr>
<td>Network Firewalling</td>
<td>Border controls for each security zone</td>
<td>$250K</td>
<td>FY15</td>
</tr>
<tr>
<td>Secure Network Engineering</td>
<td>Segment and isolate systems into differing security zones</td>
<td>$0-</td>
<td>FY16</td>
</tr>
<tr>
<td>IDS &amp; IPS</td>
<td>Intrusion detection/prevention systems</td>
<td>$200K</td>
<td>FY16</td>
</tr>
<tr>
<td>Centralized Logging</td>
<td>Improved correlation &amp; diagnostics of events</td>
<td>$50K</td>
<td>FY16</td>
</tr>
<tr>
<td>Info Security Enhancements</td>
<td>Tools for improved auditing and incident response</td>
<td>$60K</td>
<td>FY16</td>
</tr>
</tbody>
</table>
UMS Response – Cost Summary

• One-time costs:
  FY14  $ 50K
  FY15  310K
  FY16: 310K
  Total: $ 670K

• Recurring costs:
  Maintenance $ 162K
  Salary & Benefits (3 FTE) $ 270K
  Total $ 432K
Future Initiatives for Information Security

- Presidio offered future ideas, including:
  - Campus-level server protection
    - e.g. HVAC servers, active directory controllers
  - External exposure of devices
    - e.g. workstations, printers, mobile devices
  - Changing world
    - PCI 3.0
Summary

• Presidio provided 27 findings

• IT developed a plan with 9 initiatives
  • $670K one-time expenses
  • $432K recurring costs
  • 2+ years to implement

• Scope does not include future initiatives for information security