University of Maine System
Information Security Review

Summary

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 include 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.