

*Steve Corbató, Interim CIO, USHE and the USHE Institutional CIOs<sup>1</sup>  
August 27, 2014*

## **Current situation**

*“We are understaffed and underresourced for the level of complexity and the sophisticated adversaries that we now face daily on the IT security front.” – a USHE campus CIO, July 2014*

On a constant basis, increasingly capable and well-equipped attackers probe academic and corporate computer networks around the world for vulnerabilities to exploit. These attackers have a variety of motivations – financial gain, identity theft, harvesting detailed personal information, or stealing valuable research or clinical data. Specialized information technology (IT) and security professionals within these organizations attempt to thwart these malicious activities daily, and the small cadre of experts within the Utah System of Higher Education (USHE) are no exception.

At the USHE institutions, literally thousands of attempts to compromise the campus networks and their wide variety of connected systems occurs daily. As reported all too frequently in the national media, academic institutions across the U.S. have experienced significant losses of data, resources, and reputation in the wake of these attacks. Recent high-profile network breaches and the ensuing data losses at Stanford, Emory, the University of Maryland, and Indiana University among others all resulted in significant financial and reputational losses to the institutions. In these instances, the aggregate incident costs ran into the millions of dollars – to discover what happened, to repair the technical damage (if the damage can be repaired), to communicate with and to protect those in the campus community who were affected (e.g., providing credit rating services for one or more years), and to implement new systems and requirements that attempt to prevent a recurrence. In addition, the loss of protected information such as patient information or student records can result in liability for increasing fines and other penalties from the federal government.

At the recent summer meeting of USHE’s campus Chief Information Officers (CIOs) at Southern Utah University, the group made the clear determination that collectively we have reached the point where these mounting security risks call for a significant revision of our approach to computer and network security and the mitigation of the concordant risks within USHE. We recognize that like most enterprises currently, we are relatively small players in an IT ‘arms race’ with mostly unknown adversaries during a time of constrained budgets and resulting efforts for organizational efficiencies.

## **Recommendations**

Managing these growing IT risks now require that we deal with the technical sophistication and complex human factors that fall beyond that of any USHE institution’s typical organizational knowledge and expertise. We propose to approach these security risks collectively and to maximize our individual strengths in the security and privacy domain.

- Commencing in FY16, we request an increase in ongoing funding of \$2.1 million to accelerate our efforts to create more secure IT environments on all of our campuses. We propose to create the new position of USHE Chief Information Security Officer (CISO) to provide system

---

<sup>1</sup> Phil Allred, Snow; Steve Corbató, U. of Utah; Bret Ellis, WSU; Eric Hawley, USU; Gary Koeven, DSU; Tom McFarland, SUU; Ray Walker, UVU; and Bill Zoumadakis, SLCC; with participation of Ray Timothy, UEN.

oversight across the campuses and USHE itself and coordination for the individual campus security and privacy teams.

- Enhance assessments of IT security practices and vulnerabilities by engaging an external experienced team and to add to these groups selectively where required.

In addition, we propose to provide the following security and privacy related initiatives:

- Increased Focus on the Campus End User Experience and Education/Training (\$500,000)
  - Third Party Security Training & Documentation
  - Identity Finder software
  - Additional Staffing
- Strengthening Campus Perimeter Defenses (\$750,000)
  - Require Multi-Factor Authentication for critical systems containing institutional data, including student records and clinical information
  - Deploy Next Generation Firewalls
  - Add Intrusion Detection/Prevention Systems
  - Additional Staffing
- Enhancing Risk Assessment / Audit Detection (\$550,000)
  - Conduct external IT Security and Privacy Risk Assessments of all USHE campuses
  - Provide more rigorous logging of system and network events and the associated analytical tools for extracting threat and attack information from these large data archives
  - Implement a Security Incident and Event Management (SIEM) solution across USHE
  - Provide or augment Data Breach Insurance where required
- Creation of a dedicated USHE CISO position – to increase coordination among the USHE institutions and UEN, which connects all our campus networks (\$300,000)

#### **Immediate Results of Shared IT Security and Privacy Funding Request**

- Designate a **central USHE CISO** – one system-wide leader to coordinate and extend our security efforts for intrusion detection and best practice sharing.
- Provide funding for **rigorous external security assessments** at the USHE institutions on an annual basis
- **Acquire critically needed tools to improve our compliance** with standard IT security best practices

In summary, the risks associated with data breaches and other IT security failures represent some of the most significant and widely visible risks that any higher education institution faces. With this proposal to the USHE Presidents, we seek to utilize our in-state resources more effectively in the face of these growing threats and to advance our security and detection technology and processes.