Security Incident May 2012

Student Information System
University of Nebraska
Nebraska State College System

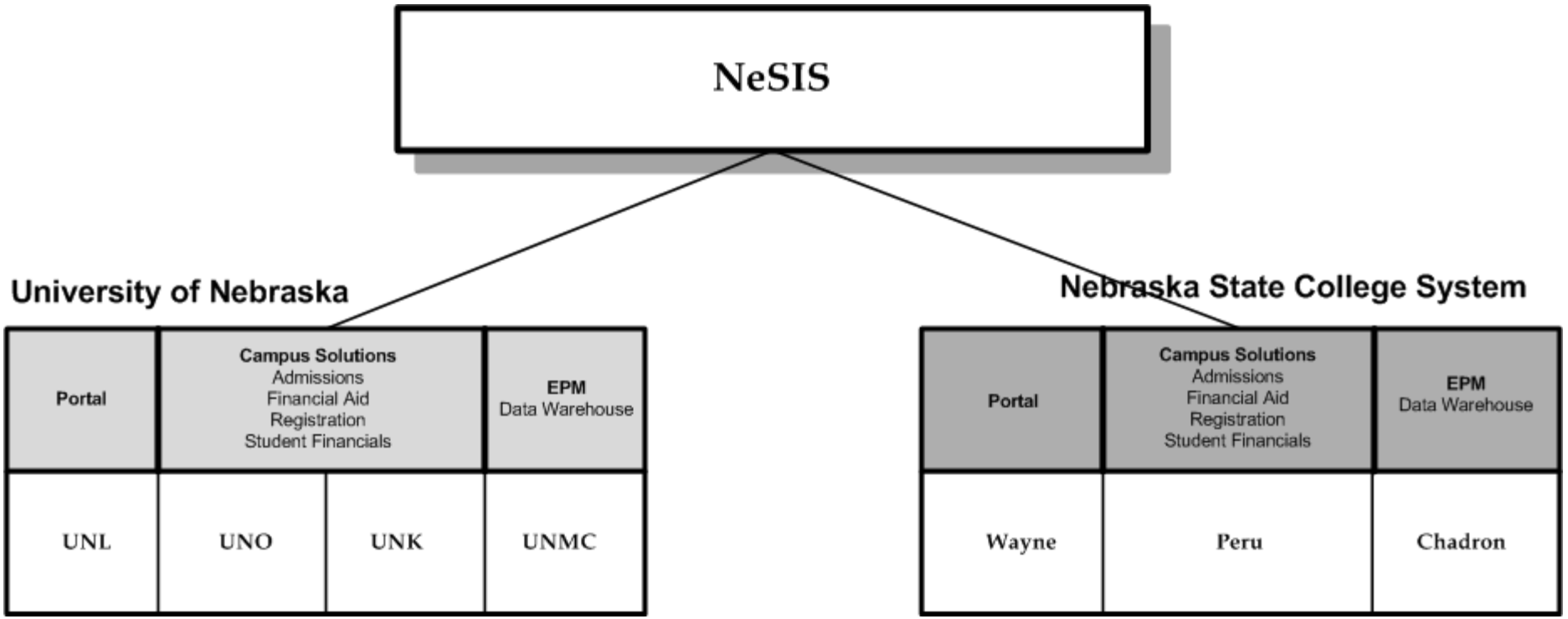
University of Nebraska

NeSIS Overview

- NeSIS has been operational for two years and is based on Oracle's PeopleSoft Enterprise Campus Solution platform
- Major components are the PeopleSoft application and the Oracle database that supports it
- UNCSN manages two complete versions, one for the University System and one for the Nebraska State College System
- NeSIS oversight: Implementation team and Steering Committee, both with representatives of all campuses and state colleges

PeopleSoft®

ORACLE®
DATABASE



- University and Nebraska State College Student Information Systems are two autonomous and separate systems
- Both systems were targeted as part of this breach

Incident Overview

May 23, 2012

- 10:00 p.m. UNCSN staff received an error message in PeopleSoft
  - Investigated error and determined it was result of unauthorized access to the PeopleSoft application
  - Locked compromised accounts immediately and continued to monitor the application

May 24, 2012

- UNCSN staff continued investigation and determined that individual had breached the Oracle database for the University system
  - UNCSN blocked access to the database within minutes of this discovery
- UNCSN immediately began a comprehensive investigation, including whether there were attempts to compromise the Nebraska State College database
  - Police report was filed with UNL Police at 1:10 p.m.
  - UNCSN began implementing preventive measures in response to the attack method

University of Nebraska

Response / Action Steps to Date

May 23 – Unauthorized activity within application initially detected

May 24 – Breach of database confirmed, law enforcement contacted

May 25 – News release on breach, web site established

May 26 – Email notification to individuals with bank accounts associated with NeSIS account (22,000)

May 27 – Employee and parent data identified in breached database

– News release issued on employee/parent data;

May 29 – External security experts on-site to assist in investigation

– Email notification sent to current employees (12,000)

– Letters sent to individuals with bank accounts with no email address on file or invalid email address

UNCSN Security and Technical staff have continued its investigation into the breach since May 24th to determine attack path, impact and provide assistance in the police investigation

Response / Action Steps to Date

May 30 – News release issued that individual believed responsible identified and computers seized

– Email notification sent to all current students (53,000)

May 31 – June 1 – UNO and UNL alumni associations sent email notifications to 57,000 past students since 1985/86

June 1 – Toll-free call center established; news release issued on call center

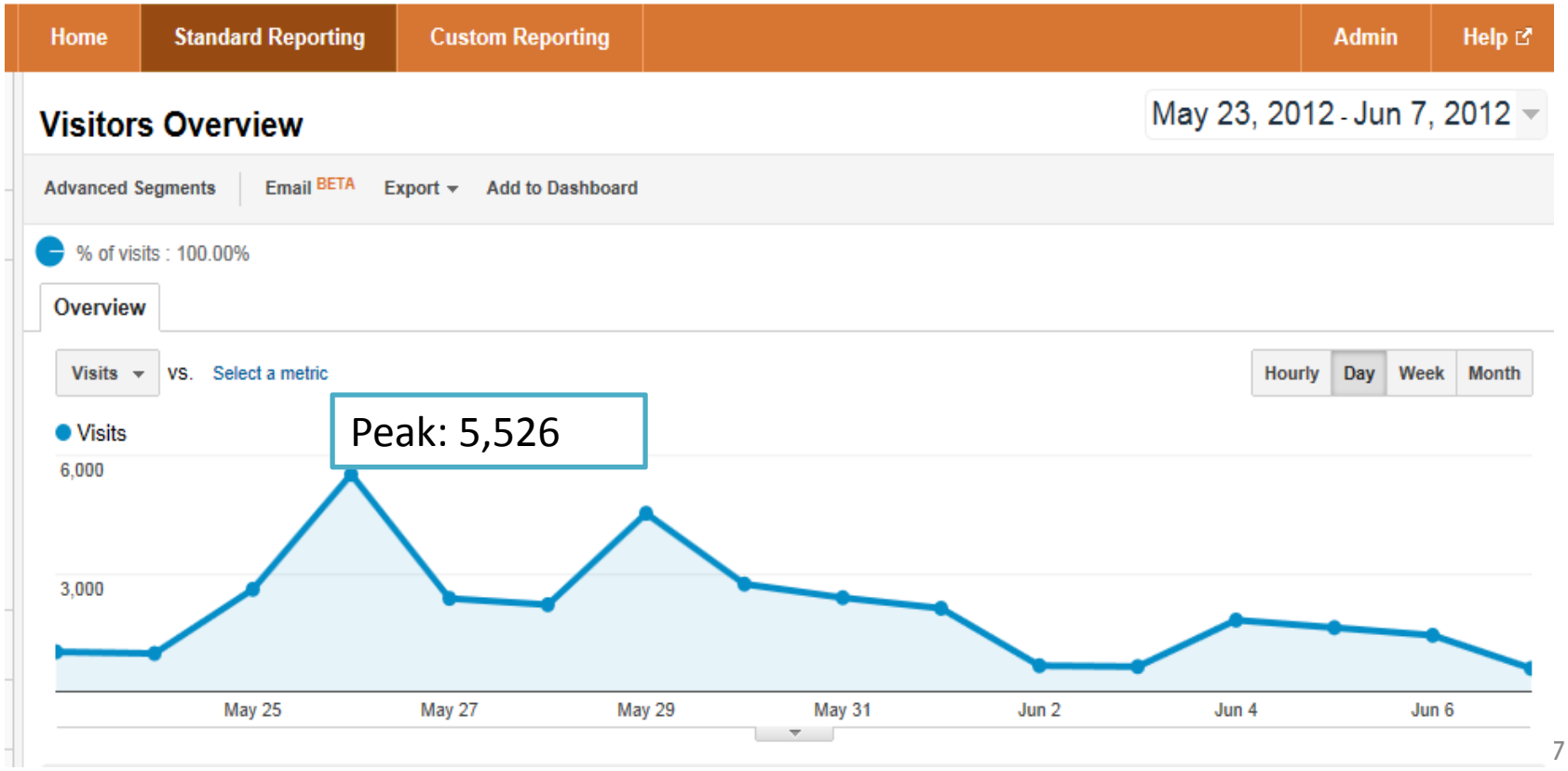
Jun 2 – June 6 – Database analysis to build additional email lists for applicants, parents, past students

June 7 – June 8 – Email notification process being finalized for remaining individuals in database with an email address

UNCSN Security and Technical staff have continued its investigation into the breach since May 24th to determine attack path, impact and provide assistance in the police investigation

Public Response

- Received over 250 questions and comments through website submission
- Received 656 calls to call center through June 7th
- Web traffic peaked the first four days and has decreased



University of Nebraska

Next Steps

- Continue to analyze this incident
  - Determining specific method and full extent of the incident
  - Continue to assist in police investigation
- Analyze and refine our response plan
- Analyze our overall information security posture
  - Assess current information security controls compared to industry best practices
  - Partner with external security firm to provide recommendations to prevent and limit the impact of future incidents

University of Nebraska

- Questions?