



Laptop on the Run – Metropolitan State College of Denver implements Business Controls' MySafeCampus system in response to stolen laptop

Situation

In early March 2006, a laptop computer containing names and social security numbers of more than 93,000 current and former Metropolitan State College of Denver (Metro State) students was stolen from the home of an employee. The employee had been using the unencrypted data to write a grant proposal and his master's degree thesis. Naturally, Metro State's immediate concern was that the students would become victims of identity crime, so they immediately reported the theft to the police.

The next looming issue was how best to communicate the incident to the student population. Since the records dated back to 1996, many of the students had graduated, and many had left the Denver area. Metro State needed a fast, efficient way to reach these people, answer their questions, and allay their fears about the loss of their personal data.

Solution

Because this was the first time Metro State had encountered such a potentially catastrophic theft, the assistant vice president of communications requested help from her colleague and counterpart at the University of Northern Colorado (UNC) who had a similar experience with vital data loss. The UNC colleague urged her to contact Steve Foster of Business Controls, Inc.

The first step was damage and rumor control. Business Controls strategized with Metro State officials, supporting an already

planned press conference to get the information out to the affected students and the public. The press conference stressed transparency and accountability from the outset, to deflect any potential accusations of a cover-up.

Within hours, Business Controls had implemented and publicized two custom toll-free MySafeCampus hotlines and worked with Metro State officials to develop a script, which included questions and answers for the hotline operators. The Web-based hotline featured frequently asked questions and custom reporting fields. This hotline was linked to the Metro State Web site as well.

Metro State also sent customized letters to each of the 93,000 affected people explaining the situation in detail and directing them to the hotline for follow-up information.

The day after the press conference, the hotline peaked at 516 calls; on the peak reporting day, 424 reports were filed. The most common questions, understandably, were "Was my name on the list?" and "Was my identity stolen and used illegally?"

As part of its three-month comprehensive audit of Metro State's network infrastructure and databases, Business Controls determined the employee was not at fault, but found Metro State's IT policies and procedures left open many security threats. Business Controls delivered a detailed report of areas to secure sensitive information about faculty, staff and alumni

and recommended tighter restrictions on employee access to data, mandatory data encryption, stronger password requirements, and shorter session time-out intervals.

And Rule number one: social security numbers may no longer be downloaded to laptops.

Result

As a result of Business Controls' recommendations, the Metro State IT department began scanning laptops for confidential data, starting with those used by employees who have access to the data network. They followed by scanning desktop computers of all faculty and staff. Authorized confidential data found on those computers will be encrypted; unauthorized data will be removed. Extensive revisions to the data management policies and procedures, followed by intensive training, will be completed by the end of the 2006-2007 school year.

The stolen laptop has not been recovered, but no affected student has reported a problem. Cathy Lucas, assistant vice president of communications for Metro State, stressed the value of outsourcing incident management. "Using Business Controls to conduct the assessment and staff the hotlines gave Metro State greater credibility. They were a critical component in assessing the situation and minimizing the damage. It could have been an ongoing crisis without them."