



Background:

In June 2009, representatives of North Carolina State University (NCSU) contacted Risk Management Associates, Inc., (RMA) regarding the commissioning of consulting services. RMA is a security and investigative consulting company based in Raleigh, NC, since 1988. Our services include computer and IT network security and forensic investigative analysis to both corporate and government clients around the country. Our consultants are uniquely qualified to provide the services requested having the necessary technical certifications, investigative experience, and commitment to ethical best practices in our business model. After discussions with NCSU legal counsel and administrators, the scope of work to be provided was clearly defined as follows:

- RMA would provide a critical review of the actions taken to date by NCSU to recover specific emails from the NCSU computer system.
- RMA would provide advice regarding any additional processes that might aid in the recovery of specific emails from the computer system.
- RMA would provide computer forensic investigative analysis if determined to be an appropriate tool to aid in the recovery of any specified emails.
- The primary focus of services provided by RMA was to evaluate the effort to locate and assist in locating not previously recovered emails from the jlobie@ncsu.edu email account regarding the hiring of Mary Easley.

The Office of Information Technology was directed to provide any and all necessary support and access to RMA during all phases of this review. All requests for information related to email accounts, network setup and configuration, policies and procedures, reports, and actions by NCSU were made immediately available to RMA consultants. The OIT staff was found to be extremely conscientious in their efforts to comply with the direction to assist RMA with conducting this independent review.

Methodology:

After evaluating the scope of work, RMA met with the Director and staff of the OIT to review the steps taken to date to comply with the various requests regarding the emails in question. Consultants toured the facilities and made observations regarding the overall network security and related physical security measures in place at the University to safeguard the information stored and maintained in their network. RMA requested and received documents regarding the operation of the OIT, their policies and procedures (specifically policies and procedures related to complying with “legal holds” on data), as well as their previous efforts to locate the emails in question. The critical review of these processes, the capabilities and resources available to the OIT staff in their efforts to comply with the various requests, and their ability to demonstrate a transparent unambiguous effort was the objective of our inquiry.

Findings:

Network and Physical Security

Consultants found that the physical security and access control measures in place at the location of the IT Network facility were adequate to restrict access to the system and to identify those who have authority to access the systems observed. The security software and IT security intrusion measures/countermeasures in place provide the necessary security to prevent and detect efforts to compromise the system.

Imbedded Issue

As detailed in the letter to the United States Attorney's Office dated June 24, 2009, the University initiated a process to preserve, recover, and provide an assortment of documents and emails to both the media by way of a "public documents request" and to the government in response to a Federal Grand Jury subpoena. This letter provides a summary of the efforts made by the University to implement their policies and procedures regarding those requests and the subsequent imbedded issue that arose when Mr. Campbell provided emails he had received from Dr. Oblinger's "priority" email account that were not previously submitted by the University (see attachments). This matter formed the basis for not only the additional efforts made by the University's OIT to locate those emails, but the engagement of RMA to provide an independent review of those efforts and computer forensics services.

The emails in question were from a time period between January and June of 2005. RMA reviewed the actions taken by the OIT to locate, recover and provide the emails.

Subsequent to Mr. Campbell's disclosure of emails that he had stored on his hard drive, the University instructed the OIT to search through any archived records and/or data storage tapes that could be located to determine if there were any possible records from that time period. OIT routinely makes copies of Groupwise post offices in response to what are referred to as "legal holds." These legal holds are basically backups of all of the data in the specified server related to any kind of request to preserve such data in response to possible legal/administrative matters. They are normally for specific time periods and involve specific information, emails, or documents being requested. One such "legal hold" for the period of time in 2005 was located in the storage area for those items. The tape was dated 9/3/2005. It had been inadvertently saved after the actual incident under evaluation was disposed of and existed only because of that oversight. It was discovered and brought forward due the diligence of the OIT to assist in locating and complying with the instructions from the University.

Using sophisticated processes, the OIT was able to restore that information in a network environment that allowed them to search for the emails in question. There were a number of emails in the restored jlobie@ncsu.edu account prior to 9/3/2005. They were able to locate some previously undiscovered emails, but not all of those provided by Mr. Campbell. Those emails were not on the server at the time that the backup tape was made on 9/3/2005. There is no data available to indicate how the emails were deleted or by whom and what process. Groupwise emails are stored on a server and only saved to a user's workstation if saved by the user. There is no indication that this was the case. Email servers at NCSU have gone through a number of hardware and software updates since 2005. It is the opinion of RMA that the University and the Office of Information Technology has done everything technically possible to recover all emails from the priority Oblinger email account, and that there is nothing to suggest that their efforts were anything less than totally compliant with their policies and procedure as well as the spirit and intent of the requests that have been made.

Hard Drive

Dr. Oblinger (or others) could have saved the emails in question to the desktop computer or laptop computer hard drives in use at the time of the activity. RMA requested that the University locate the desktop computer and any laptop used by Dr. Oblinger. It was determined that the desktop computer hard drive in use in 2005 was reissued prior to any requests for emails or documents. The hard drive was "scrubbed" of all data before being reformatted and issued to the new user. The practice of completely removing the historical information from a reissued hard drive is suggested best practices to ensure that any confidential, proprietary, and protected information is not compromised. The laptop used by Dr. Oblinger in 2005 was recovered by RMA consultants and forensically examined. There was no evidence found in either the active files or previously deleted forensically recovered files of the existence of the emails in question. This is because the laptop may not have been used to create the emails or the emails were not saved by the user on the laptop hard drive, but remained stored in the client account on the server until deleted.

Conclusions:

After reviewing the facts and circumstances surrounding the efforts of NCSU to comply with the requests for the public documents in question and in their efforts to be fully compliant with the direction of legal counsel to preserve and provide information pursuant to the various subpoena, it is the opinion of RMA consultants that University has done everything technically possible to comply.

- RMA consultants interviewed administrators involved in that process and the OIT staff responsible for the recovery and preservation of the information. They were found to be technically competent. It is also the opinion of RMA consultants that they performed their duties and responsibilities with the appropriate oversight and integrity necessary to ensure the credibility of the resulting data/information provided.

- RMA consultants also found that the processes (policies and procedure) in place at the time of these various requests were appropriate to demonstrate compliance with eDiscovery requests made at that time and that they were followed by the University and the assigned staff.
- RMA consultants found that the technical approach taken by the University and the assigned staff was sound. In fact, the measures taken to rebuild a server environment long since discarded for newer technology to review the September 3, 2005, “backup tape” demonstrated this expertise and commitment to getting to the bottom of this issue. Not only were individual email accounts archived but the Groupwise Post Office that contained that email account was archived. User network data folders, network share folders, and workstations were also copied. Several departments worked with the Office of Information Technology to accomplish these tasks, including Groupwise Email Services and Client Services. When RMA suggested the use of computer forensics to examine the hard drive of Dr. Oblinger, he immediately made the computer available to consultants.
- The deletions of the jlobie@ncsu.edu emails for the period January 2005 to June 11, 2005, occurred prior to September 3, 2005.
- RMA’s efforts independent of the work done by the NCSU OIT recovered no additional emails from the jlobie@ncsu.edu account for the period January 2005 to June 11, 2005.

As previously mentioned, North Carolina State University and the Office of Information Technology take the collection and preservation of data very seriously. In this case, the University blended the effective use of the technology with appropriate policies and procedures with technically skilled people whose high degree of integrity and professionalism was evident to the consultants.

June 24, 2009

Mr. John Bruce
Mr. Dennis Duffy
U.S. Attorney's Office - EDNC
310 New Bern Avenue
Federal Building, Suite 800
Raleigh, NC 27601-1461

Re: N.C. State University Grand Jury Document Subpoena Response

Dear John and Dennis,

On behalf of N.C. State University, and in continuing response to those three document subpoenas dated May 19, 2009 and addressed to N.C. State University Custodian of Records, N.C. State University Provost Larry Nielsen (official capacity), and N.C. State University Chancellor James Oblinger (official capacity), we submit the enclosed disc containing copies of documents from the following sources:

- Documents from the Chancellor's Office: NCSU-CO-0001479 to NCSU-CO-0001575
- Documents from the Provost's Office: NCSU-PO-0002557 to NCSU-PO-0003012
- Documents from the Vice Chancellor for Finance and Business: NCSU-VCFB-0008000 to NCSU-VCFB-0008022
- Documents from the College of Humanities and Social Sciences: NCSU-CH-0006134 to NCSU-CH-0006369
- Documents from Board of Trustees Member John Sall: NCSU-BOT-JS - 0009000 to NCSU-BOT-JS - 0009023

You will see that we produce e-mails from the files of the person sending the e-mail, but often don't produce copies of those e-mails from the files of the recipients. During much of the relevant period the e-mail retention policy at N.C. State required the sender of an e-mail to retain it but did not require the recipient to retain copies, whether direct recipient or copied recipient. The present retention policy requires retention of all e-mails.

Also as we have discussed, as Chancellor, Dr. James Oblinger had two e-mail accounts. The first, James_Oblinger@ncsu.edu, was published on the N.C.S.U. website and was the primary mailbox for general e-mail. The second e-mail account, Jlobie@ncsu.edu, was managed directly by Dr. Oblinger and used for higher priority items and quicker response. This second account was opened in early January 2005 when Dr. Oblinger became Chancellor.

Letter to U.S. Attorney's Office

June 24, 2009

Page 2

In collecting documents responsive to these grand jury subpoenas, we discovered no documents on the Jlobie@ncsu.edu account prior to June 11, 2005. We know this account was in use from its opening and have been unable to determine how and why the e-mails sent from and received by this e-mail account during this time period were deleted. As soon as we discovered this, we instructed N.C. State University technology personnel to do everything possible to reconstruct deleted documents from this account for this time period. I enclose a detailed statement of steps taken by N.C. State University personnel to recover e-mails from that account.

In this process a substantial number of e-mails were recovered and they are included in the documents produced today. However periods of time remain between January and June, 2005 for which thus far we have been unable to recover records from this account. We have retained the services of an IT forensic expert who is presently working to take all possible steps to recover these documents. We will produce to the grand jury all responsive documents recovered and we will make all others available as public records.

As with our production of June 8, 2009, we are continuing to review records of N.C. State University and collect documents responsive to these subpoenas. Those documents will be produced promptly as they are identified and collected.

As always, please call if you have any question concerning any of these matters.

Yours truly,
McMillan Smith & Plyler

A handwritten signature in black ink, appearing to read "STEVE" in a stylized, cursive font.

Stephen T. Smith

**Process used to recover e-mail related to Mary Easley
for the time frame of April-July of 2005**

Retention Policy

University policy is that the individual is responsible for maintaining records following the retention policy (<http://www.ncsu.edu/policies/informationtechnology/REG08.00.9.php>). The University only keeps deleted, sent or inbox messages for 180 days in a user's live mailbox. After 180 days, messages are either automatically deleted or archived depending on the user's mailbox settings. Messages that are archived are kept forever. Backups of the mail system are kept for 90 days for Disaster Recovery purposes. Any backups kept longer than 90 days would only be for a requested litigation hold on a specific user's mailbox. These backups retained longer include a copy of the "Post Office" containing the specific user.

On January 22, 2009, the University launched an email retention team to develop a plan and any policy updates for the email retention policy in order to comply with Executive Order No. 150 – Email Retention and Archiving as well as the eDiscovery law. The revised draft policy is in process.

James Oblinger's Email Accounts

Dr. James Oblinger has two email accounts. The first is published on the website and is the primary mailbox for general email (james_oblinger@ncsu.edu). The second email account (jlobie@ncsu.edu) is managed directly by Dr. Oblinger and provided for higher priority items and quicker response. Proxy email access to the general email account was held by most members of the chancellor's office staff. Only Dr. Oblinger had access to the second email account.

Previous Public Records Requests

Prior to the subpoena requests there were at least three records requests specifically related to the hiring of Mary Easley, all three from the media. The first request related to her change in pay in 2008. In response, paper files were reviewed and keyword searches were performed on the word "Easley" on the above accounts and that of PJ Teal (pj_teal@ncsu.edu).

The second and third requests asked for documents related to the 2005 hiring of Mary Easley, including the Board of Governors submission packet, Board of Trustees meeting minutes, her offer letter, etc. The same keyword search was conducted and all

responsive documents produced. Multiple staff members in the chancellor's office were involved in reviewing and copying the files.

File Preservation

On May 26, 2009, the Office of Information Technology (OIT) received a notice from NC State General Counsel that all records regarding the hiring of Mary Easley needed to be preserved because of the Federal Grand Jury Subpoenas received by the university. OIT staff spent the next 3 days archiving email accounts and copying file systems and computer disks for the individuals that might have information relating to this event. This was completed by May 29, 2009. Several subsequent notices to preserve information regarding the hiring, promotions and salary of Mary Easley were distributed to various individuals (5/29, 6/8, 6/10, 6/16) in which the OIT staff completed the preservation for all requested individuals by June 19, 2009.

Missing Email Search

On or about June 2, 2009 paper copies of additional email between James Oblinger (jlobie@ncsu.edu) and McQueen Campbell (off campus account), occurring in 2005 and relating to the hiring of Mary Easley were delivered to the university. Chancellor's office staff reviewed the jlobie@ncsu.edu email account and determined that this mailbox did not contain any email prior to June 2007. Marc Hoit, VC for Information Technology (CIO), was contacted on June 4, 2009 and asked for any backup files that would contain these earlier emails. OIT's preliminary determination was that existing back up files did not contain any additional email.

On June 5, 2009, the CIO contacted the GroupWise (Email system) tech and asked them to see if they could look through backup files and find mail in the jlobie@ncsu.edu account prior to mid June 2005. The CIO was informed that the oldest tape that could be found, according to the litigation hold records, was from 2006 and probably would not have sent or deleted messages from June 2005 or earlier.

On June 8, 2009, the CIO was asked to further investigate and see if there were any files with older messages. The vault was physically searched for tapes backed-up beyond 2006; this was coordinated by the OIT Director for Security and Compliance. In this search, tapes dated 9/3/05 were found in the vault, but the format could only be read by an old server and tape drive that was no longer being used. In order to read these tapes the older server, tape drive, and software had to be brought online in order to determine if recovery of the data was possible. This hardware configuration was initiated.

On June 9, 2009, OIT was also asked to restore the email account for Andy Willis (lawillis@ncsu.edu) as some of the Oblinger/Campbell email was copied to Willis. It was determined that this account was still active and it had saved mail back to 2003. Several existing chancellor's office staff members (dfbaker, fmmilks and jawill12) still had access to the account. The account was also forwarding mail to the account held by Willis at UNC-General Administration. The University disabled all access to the account and stopped forwarding after consulting with Willis. The evening of June 9, 2009 Charles Leffler was given read only access to the Willis account. The IT manager found that the year 2005 and some 2006 email was missing from the live account. Access logs were checked to see if any data had been recently changed which it had not. The University loaded the June 1, 2009 backup of the current mail to see if the year had been deleted recently. The data was the same as the current account.

Configuration of the old server/tape environment was completed the end of day on June 10, 2009. The tapes dated 9/3/05 were retrieved from the vault on the morning of June 11, 2009 and the tapes were successfully cataloged. It was discovered that GroupWise Post Office 6 (PO6) was on the tapes. PO6 was believed to be where Mr. Willis' mailbox and the Oblinger's mailbox (jlobie) were stored. On June 12, 2009, the OIT staff resurrected the server/tape environment and began the restore/mailbox configuration process, which was completed on Sunday evening, June 14, 2009. Leffler was given read only access to data retrieved for lawillis@ncsu.edu , pjteal@ncsu.edu and jlobie@ncsu.edu mailboxes on June 15, 2009.

This restoration included the time period prior to September 3, 2005 and included additional email concerning the Mary Easley employment. A general search of these email records was done by keywords and specifically the time period of April 27, 2005 through May 19, 2005. All responsive email was produced for submission.

The University also looked into the original configuration of Dr. Oblinger's email account. There was not any tracking record, but one email describing the set up of the email account when he moved from Provost to Chancellor. There is no record to confirm how messages from 2005 became missing. It is speculated that these were deleted as part of routine mailbox cleanup and were beyond backup time periods. James Oblinger, Andy Willis and PJ Teal all received their Blackberry devices on April 11, 2005 and there appeared to be issues with initial delete settings.