ANDERSON COUNTY SERVER UNAUTHORIZED ACCESS INVESTIGATION **OCA#1608030030**

BRIEF REPORT SUMMARY **REPORT STATUS: CLOSED PENDING MONTHLY CHECKS OF CRIMINAL ACTIVITY RELATING TO THIS CASE SUCH AS FRAUD OR IDENTITY THEFT**

NOTE: THIS SUMMARY IS NOT ALL INCLUSIVE AND ONLY CONTAINS A SUMMATION OF MAJOR POINTS OF INTEREST PERTAINING TO THIS REPORTED INCIDENT. THIS SUMMARY SHALL ALSO INCLUDE BRIEF EXPLANATIONS AS TO HOW THE INVESTIGATION CONTINUED FROM INITIAL COMPLAINT TO CURRENT DATE. SOME ITEMS TAKEN VERBATIM FROM MY ORIGINAL REPORT.

08/03/2016:

THE HUMAN RESOURCES DIRECTOR, RUSSELL BEARDEN INITIATED A COMPLAINT AT THE ANDERSON COUNTY SHERIFF'S OFFICE, ALLEGING THAT HE BELIEVED THAT UNKNOWN INDIVIDUALS HAD GAINED ACCESS TO THE ANDERSON COUNTY GOVERNMENT MAIN AND/OR BADGE ACCESS SERVERS AND POSSIBLY OBTAINED, REMOVED OR ALTERED DATA. HE ALLEGED THAT THIS UNAUTHORIZED ACCESS OCCURRED ON MORE THAN ONE OCCASION STARTING ON THE NIGHT OF 05/20/2016 AND CONTINUED TO MID-JULY 2016. HE STATED IN HIS COMPLAINT THAT SOME OF THE SERVER SYSTEM LOGS HAD BEEN DELETED AND HE FURTHER ASSERTED THAT THERE WERE LARGE GAPS IN THE LOGGING ASPECT OF THE SERVERS.

BRIAN YOUNG (CO-INVESTIGATOR FOR TECHNICAL KNOWLEDGE) WAS INTERVIEWED AND HE CONCURRED WITH RUSSELL BEARDEN. BRIAN YOUNG ADVISED THAT HE WAS ASKED BY BEARDEN TO ASSIST WITH THIS ISSUE. MR. YOUNG ADVISED THAT HE EXAMINED THE NTSF FILE LOG AND THE WINDOWS EVENT REGISTRY AND SUBSEQUENTLY COPIED THE FILES INTO A TEXT FILE ONTO A THUMB DRIVE SO THAT HE COULD EXAMINE THE REGISTRY AND NTFS LOGS. MR. YOUNG STATED THAT HE FOUND LARGE GAPS IN THE FILES WHERE NOTHING WAS READING/WRITING TO ANY FILES. MR. YOUNG FELT THAT IT APPEARED AS THOUGH SOMEONE HAD SIMPLY TURNED OFF THE SYSTEM. MR. YOUNG WAS CONCERNED THAT LARGE AMOUNTS OF DATA MAY HAVE BEEN EX-FILTRATED FROM ANDERSON COUNTY SERVERS.

DUE TO THE EXTREMELY TECHNICAL ASPECTS OF THIS CASE, I REQUESTED TO RETAIN BRIAN YOUNG'S SERVICES AS A CO-INVESTIGATOR IN THIS CASE. DURING THIS INVESTIGATION, BRIAN YOUNG IS TO REPORT TO ME AS NEEDED. BRIAN YOUNG WAS SUBSEQUENTLY RETAINED BY ANDERSON COUNTY GOVERNMENT FOR THE PURPOSE OF REBUILDING THE NETWORK, SERVERS, EMAIL, AND ANY OTHER I.T. ISSUE NEEDED BY THE COUNTY.

BRIAN YOUNG WAS ASKED TO SUBMIT A RESUME LISTING HIS EXPERIENCE, SKILL ABILITIES AND A REFERENCE LIST. AFTER MR. YOUNG COMPLIED WITH THE REQUEST, I CONTACTED SEVERAL REFERENCE LISTINGS. NONE OF THOSE PERSONS LISTED GAVE A NEGATIVE INDICATION AS TO MR. YOUNGS ABILITIES AND SERVICE TO THEIR BUSINESSES. IN FACT, ALL PERSONS INTERVIEWED GAVE A HIGH RECCOMMENDATION OF BRIAN YOUNG.

WITH THE INFORMATION RECEIVED BY BOTH RUSSELL BEARDEN AND BRIAN YOUNG, IT WAS DETERMINED SUFFICIENT INFORMATION WAS PRESENTED TO WARRANT A CRIMINAL INVESTIGATION FOR THE FOLLOWING OFFENSE:
T.C.A. 39-14-602 COMPUTER OFFENSES…… (FOR MONETARY GAIN GRADED AS T.C.A. 39-14-105, CLASS OF THEFT -OTHERWISE, UNAUTHORIZED ACCESS IS CLASS C MISDEMEANOR)

IT WAS LEARNED AT THE ONSET OF THIS INVESTIGATION, THAT ANDERSON COUNTY GOVERNMENT HAD A CONTRACTED I.T. VENDOR FOR THE UPKEEP AND GENERAL HEALTH OF THE ANDERSON COUNTY COMPUTERS, SOFTWARE AND SERVERS. I WAS ADVISED BY RUSSELL BEARDEN THAT THE CONTRACTED I.T. VENDOR HAD AN ASSIGNED TECHNICIAN TO OVERSEE AND ADDRESS ISSUES. MR. BEARDEN WENT ON TO SAY THAT THE PROGRAM "LOGMEIN",USED TO REMOTELY CONTACT THE SERVERS, CONTAINED IDENTICAL USERNAME AND PASSWORDS, WHICH MOST EMPLOYEES HAD COMMON KNOWLEDGE OF. WITH THAT INFORMATION I DECIDED TO ADVISE FINANCE DIRECTOR NATALIE ERB THAT SHE SHOULD CONSIDER ADVISING EMPLOYEES AND THE CONTRACTED I.T. VENDOR TO REFRAIN FROM USING "LOGMEIN". MS. ERB DID SEND AN EMAIL TO THE CONTRACTED I.T. VENDOR TO CEASE ALL

ACTIONS WITH ANDERSON COUNTY COMPUTER SYSTEMS SO THAT NOTHING COULD BE ALTERED DURING THIS INVESTIGATION.

I MET WITH F.B.I. CYBER-CRIMES DIVISION AGENTS, AGENT RICHARD LARA AND AGENT SCOTT WENGER. IT WAS DETERMINED EARLY ON, TO REQUEST F.B.I. ASSISTANCE IN CASE THIS REPORTED INCIDENT MET THE REQUIREMENTS FOR THE F.B.I. TO TAKE OVER THIS CASE.

I RECOGNIZED THAT THE FIRST PRIORITY IN THIS CASE WAS TO DETERMINE IF, IN FACT, AN ACTUAL UNAUTHORIZED ACCESS OR INTRUSION OF THE ANDERSON COUNTY GOVERNMENT SERVERS HAD OCCURRED. THE ONLY WAY TO DETERMINE THE VALIDITY OF THE ORIGINAL COMPLAINT WOULD BE TO EXAMINE THE SERVERS, HARD DRIVES, AND ANY OTHER MEDIA THAT WOULD YIELD SAID INFORMATION. IT WAS ALSO DISCUSSED THAT MY INVESTIGATION SHOULD FOCUS ONLY ON THE ACTUAL REPORTED UNAUTHORIZED ACCESS.

08/04/2016

INITIAL IMAGING OF SERVER DRIVES:

WITH THE ASSISTANCE OF THE F.B.I., A LIVE MEMORY CAPTURE AND DRIVE IMAGE WAS CONDUCTED ON THE MAIN SERVER FOR ANDERSON COUNTY GOVERNMENT, SAID CAPTURE AND DRIVE IMAGE WAS COPIED TO A FORENSICALLY FORMATTED WESTERN DIGITAL 3TB HARD DRIVE. A LIVE IMAGE CAPTURE AND A DRIVE IMAGE IS AN EXACT FORENSIC COPY OF NOT ONLY DATA ON A HARD DRIVE, BUT ALSO OF PROCESSES IN USE AND OF RAM STORED DATA AND NTFS FILES. THE COPY IS EXACTLY AS THE ORIGINAL DRIVE.

08/05/2016

TRANSPORT OF DRIVES TO TBI

I HAND DELIVERED THE LIVE MEMORY CAPTURE/DRIVE IMAGE AS WELL AS SMALL THUMB DRIVE WHICH HAD BEEN PRESENTED TO ME BY BRIAN YOUNG DURING HIS INITIAL INTERVIEW TO TBI IN NASHVILLE. THE THUMB DRIVE CONTAINED THE NTFS FILES THAT MR. YOUNG HAD INITIALLY EXAMINED.

H.R. DIRECTOR RUSSELL BEARDEN REPORTED THIS INCIDENT BY INFORMING ALL ELECTED OFFICIALS AND DEPARTMENT HEADS THAT THERE WAS A “SYSTEM-WIDE BREACH OF OUR MAIN COURTHOUSE SERVER. THE EXTENT, TYPE AND AMOUNT OF DATA COMPROMISED HAS NOT YET BEEN FULLY DETERMINED”.

08/07/2016:

EMPLOYEE CREDIT UNION REPORTS OF COMPROMISED ACCOUNTS:

RECEIVED INFORMATION ADVISING THAT THERE WERE REPORTS OF TWO EMPLOYEE’S CREDIT UNION ACCOUNTS THAT HAVE BEEN COMPROMISED. IN AN ATTEMPT TO OBTAIN THE NAMES OF THE TWO “VICTIMS”, SGT. DAVIS WAS ADVISED THAT THAT INFORMATION COULD NOT BE PROVIDED BECAUSE OF CONFIDENTIALITY ISSUES**.**

08/08/2016:

FOLLOW-UP TO CREDIT UNION:

SGT. JEFF DAVIS AND I PROCEEDED TO KNOXVILLE TEACHER’S CREDIT UNION (K.T.C.U.) TO DETERMINE HOW BADLY THE CREDIT UNION ACCOUNT HOLDERS HAD BEEN AFFECTED. I INTERVIEWED JIM SANDERSON OF THE K.T.C.U., ROOM #123 OF ANDERSON COUNTY COURTHOUSE, AND ASKED HOW MANY REPORTS THE CREDIT UNION HAD RECEIVED FROM ACCOUNT HOLDERS REGARDING THE THEFT OF THEIR IDENTITY AS WELL AS ANY INTRUSIONS INTO THE CREDIT UNION SERVERS. MR. SANDERSON ADVISED THAT THE CREDIT UNION HAD NOT RECEIVED A SINGLE COMPLAINT, REQUEST FOR RE-IMBURSEMENT, OR ANY OTHER CALLS REGARDING EMPLOYEE ACCOUNTS BEING COMPROMISED OR OF ANY ISSUES OF IDENTITY THEFT.

08/09/2016:
RESPONSE FROM TBI:
I RECEIVED AN EMAIL (DATED 08/08/2016) FROM TBI AGENT J. REEVES GARNETT. AGENT GARNETT WROTE THAT HE EXAMINED SOME OF THE COMPUTER LOGS FROM THE IMAGE OF THE BADGE SERVER. AGENT GARNETT ADVISED THAT HE OBSERVED NUMEROUS "LOGMEIN" ACTIVITIES THAT HE ASSUMED WERE SUSPICIOUS, BUT ADDED THAT THE ACTIVITY COULD BE LEGITIMATE. AGENT GARNETT ADVISED THAT TBI WAS NOT EQUIPPED TO COMPLETE MY REQUEST OF CONDUCTING A FORENSIC SEARCH OF THE LIVE MEMORY CAPTURE AND DRIVE IMAGE TO LOOK FOR EVIDENCE OF HACKING TO INCLUDE DATA ALTERING VIRUS IMPLEMENTATION AND DATA EX-FILTRATION**.** AGENT GARNETT PROVIDED ME WITH AGENCY INFORMATION UNDER THE DEPARTMENT OF HOMELAND SECURITY.

I CONTACTED TBI AGENT JOEL WADE ABOUT THE LIVE MEMORY CAPTURE AND THE RESULTS OF TBI'S EXAMINATION OF THE SUBMITTED ITEMS. AGENT WADE ADVISED THAT TBI HAD ONLY EXAMINED THE SUBMITTED THUMB DRIVE. IT WAS DETERMINED THAT THE DEPARTMENT OF HOMELAND SECURITY WAS THE BEST COURSE OF ACTION TO CONDUCT AN OFFICIAL FORENSIC REVIEW OF ITEMS RELEVANT TO THIS CASE.

INITIAL CONTACT WITH US-CERT:
I CONTACTED THE UNITED STATES COMPUTER EMERGENCY READINESS TEAM (US-CERT), A DIVISION OF THE UNITED STATES DEPARTMENT OF HOMELAND SECURITY, AND HAD A PHONE MEETING WITH ANALYST DAVID RASSON. I ADVISED MR. RASSON OF THE COMPLAINT THAT THE SHERIFF'S OFFICE HAD RECEIVED CONCERNING THIS CASE. I ALSO ADVISED MR. RASSON THAT THE VICTIM OF THIS REPORTED INCIDENT IS A GOVERNMENT ENTITY AND IT IS OF THE UTMOST IMPORTANCE THAT A CAUSE BE IDENTIFIED AS EXPEDITIOUSLY AS POSSIBLE. MR. RASSON ADVISED THAT US-CERT USES ANOTHER AGENCY FOR THESE TYPE OF ISSUES. THE AGENCY'S NAME IS MULTI-STATE INFORMATION SHARING & ANALYSIS CENTER (MS-ISAC). MS-ISAC IS A DIVISION OF THE DEPARTMENT OF HOMELAND SECURITY AND SPECIALIZES IN THESE TYPE OF ISSUES.

WINDSTREAM COMMUNICATIONS SUBPOENA REQUEST:
I CONTACTED "WINDSTREAM COMMUNICATIONS", THE INTERNET SERVICE PROVIDER FOR ANDERSON COUNTY GOVERNMENT, VIA PHONE. I REQUESTED TO SPEAK TO THE LEGAL DEPARTMENT FOR THE PURPOSE OF OBTAINING A SUBPOENA FOR ALL I.P. ADDRESSES THAT HAVE COMMUNICATED WITH A.C. COURTHOUSE FIREWALL THROUGH WIRED AND WIRELESS COMMUNICATION. I WAS ADVISED BY THE LEGAL DEPARTMENT THAT A SUBPOENA WOULD BE COUNTER-PRODUCTIVE BECAUSE WINDSTREAM DOES NOT MAINTAIN RECORDS OF I.P. ADDRESSES. THIS INFORMATION WAS PRESENTED TO BRIAN YOUNG FOR HIS REFERENCE.

I CONTACTED DEPUTY JUSTIN MASSENGILL, A.C.S.O. I.T. OFFICER. I REQUESTED THAT HE GO INTO THE VIDEO CAMERA SYSTEM AND SEARCH THROUGH FOOTAGE, FIRST ON DATES AND TIMES THAT CORRESPOND WITH THE DATES AND TIMES OF THE REPORTED SUSPICIOUS EVENTS TO THE ANDERSON COUNTY SERVERS TO DETERMINE IF THERE WAS ANY TYPE OF INTRUSION THAT WAS INTERNAL IN NATURE, SUCH AS FROM AN OFFICE, AFTER HOURS. I ALSO REQUESTED IF IT WAS POSSIBLE FOR PERSONS TO DELETE VIDEO FOOTAGE IN AN EFFORT TO HIDE THEIR ACTIVITIES. I THEN REQUESTED DPTY. MASSENGILL TO EXAMINE VIDEO FOOTAGE TO ASCERTAIN IF ANYONE WAS ACCESSING CERTAIN OFFICES. I ASKED DPTY. MASSENGILL TO LOOK BACK TO AT LEAST THROUGH THE MONTH OF MAY IF POSSIBLE. DPTY. MASSENGILL REPORTED THAT HE WAS ABLE TO EXAMINE FOOTAGE FROM MAY TO PRESENT. HE ADVISED THAT HE FOUND NOTHING SUSPICIOUS AND ADDED THAT HE FOUND NO AFTER-HOURS ACCESS TO ANDERSON COUNTY GOVERNMENT.

BRIAN YOUNG CONTACTED ME AND STATED THAT HE HAD A SERIOUS ISSUE TO REPORT. HE ADVISED THAT WHILE HE WAS EXAMINING THE CURRENT FIREWALL DEVICE, HE SAW THAT THE DEVICE SETTINGS WERE STILL IN DEFAULT MODE AND THAT IP ADDRESS LOGGING WAS SET AT A DEFAULT RATE TO OVERWRITE DATA EVERY 24 HOURS. HE WENT ON TO SAY THAT IN ALL ACTUALITY, SINCE THE ANDERSON COUNTY GOVERNMENT EMPLOYEES WERE CONSTANTLY USING THE SERVER AND CONDUCTING BUSINESS ON THE INTERNET, DATA WAS ACTUALLY BEING OVERWRITTEN IN A MATTER OF HOURS. HE STATED THAT THE FIREWALL WAS NOT THE MOST IDEAL PIECE OF EQUIPMENT FOR COUNTY GOVERNMENT USE. FINALLY, HE ADVISED THAT HE WOULD NOT BE ABLE TO OBTAIN IP ADDRESSES THAT HAD COMMUNICATED WITH THE SERVER DURING THE DATES AND TIMES OF THIS REPORTED INCIDENT. BRIAN ADDED THAT HE ALSO FOUND

ANOTHER FIREWALL THAT WAS PLUGGED IN AND POWERED ON, BUT THERE WERE ABSOLUTELY NO ETHERNET CABLES, OR ANY OTHER CABLES CONNECTED TO IT. HE STATED THAT THE FIREWALL IS VALUED AT AROUND $8,000.00 AND HAS BEEN SITTING IDLE, AND NOT BEING USED. BRIAN STATED THAT THE MEMORY IN THAT PARTICULAR FIREWALL WOULD HOLD ENOUGH LOGGING DATA FOR ABOUT 90 DAYS OR MORE.

08/10/2016:

INITIAL CONTACT WITH MS-ISAC:

I CONTACTED MULTI-STATE INFORMATION SHARING & ANALYSIS CENTER (MS-ISAC), SECURITY OPERATIONS ANALYST, PAUL DOCKTER BY PHONE. DURING OUR CONVERSATION I EXPLAINED THE SITUATION REGARDING THE REPORT OF REPEATED UNAUTHORIZED ACCESSES TO ANDERSON COUNTY GOVERNMENT SERVERS AND THE PROGRESS OF THE INVESTIGATION. MR. DOCKTER ADVISED THAT MS-ISAC WOULD NEED TO EXAMINE ALL OF THE SERVER DRIVES. HE ADVISED THAT THE DRIVES WOULD NEED TO BE COPIED USING ONLY FEDERALLY APPROVED SOFTWARE AND THAT THE DRIVES NEEDED TO MAKE THE COPIES WOULD HAVE TO BE FORENSICALLY REFORMATTED SO THAT THERE IS NO QUESTION ABOUT THE COPIED DATA. I REQUESTED MR. DOCKTER SEND DOCUMENTATION OF THE REQUIRED PROCESS. I LATER RECEIVED AN EMAIL FROM MR. DOCKTER. THE EMAIL INCLUDED A “FORENSIC IMAGING GUIDE”.

I EMAILED THE CONTRACTED I.T. VENDOR FOR ANDERSON COUNTY GOVERNMENT THAT A COMPLAINT WAS RECEIVED BY FROM AN ANDERSON COUNTY GOVERNMENT EMPLOYEE REGARDING AN UNKNOWN TYPE ISSUE WITH THE SERVER AND OFFICIALLY ORDERED ALL PERSONS WITH THE ABILITY TO ACCESS THE SERVER AND MANIPULATE DATA IN ANY WAY TO STOP UNTIL A CAUSE WAS DETERMINED.

I MET WITH CHIEF LUCAS AND ADVISED HIM THAT I WOULD NEED TO MAKE FORENSIC COPIES OF ALL OF THE SERVER DRIVES SO THAT NOTHING WOULD BE OVERLOOKED. I ADVISED THAT I WOULD NEED NEW HARD DRIVES OF THE SAME OR LARGER MEMORY CAPACITY. CHIEF LUCAS ADVISED THAT HE WOULD ADVISE MIA BOUNDS TO GET A P.O. FOR A BUDGETED AMOUNT FOR ITEMS NEEDED FOR THE INVESTIGATION.

I CONTACTED “SHIELD’S ELECTRONIC SUPPLY” AND ADVISED THAT I WOULD NEED FOUR HARD DRIVES 2TB EACH AS WELL AS A SATA/IDE ADAPTER SO THAT THE OLDER DRIVES CAN BE COPIED. I WAS ADVISED THAT ALL OF THE REQUESTED ITEMS WOULD BE READY FOR PICK UP BY 08/12/2016.

08/11/2016:

RESPONSE FROM KNOXVILLE TEACHER’S CREDIT UNION:

I RECEIVED AN EMAIL FROM DAVID UNDERWOOD, TRUSTEE/MANAGER OF KNOXVILLE TEACHERS FEDERAL CREDIT UNION. HE STATED IN HIS EMAIL THAT HE IS AWARE OF THE INVESTIGATION AND WANTED TO RELAY TO ME THAT THERE HAD NOT BEEN ANY ISSUES THAT HE IS AWARE OF AND HE ALSO ADVISED THAT THE CREDIT UNION SERVER IS INDEPENDENT OF THE ANDERSON COUNTY SERVER.

08/12/2016:

INITIAL PICK UP OF HARD DRIVES FOR COPYING:

AFTER PICKING UP FOUR(4) WESTERN DIGITAL HARD DRIVES FROM KNOXVILLE I PROCEEDED BACK TO MY OFFICE AND BEGAN THE LENGTHY PROCESS OF PERFORMING A FORENSIC FORMAT ON EACH DRIVE AS PER PROCEDURE DICTATED BY MS-ISAC. DUE TO THE SIZE OF EACH DRIVE FORMATTED, THE PROCESS TOOK ALMOST 24 HOURS FOR EACH HARD DRIVE. DRIVES COULD NOT BE COPIED UNTIL ALL NEWLY PURCHASED DRIVES COULD BE FORMATTED. AFTER ALL DRIVES WERE FORMATTED BRIAN YOUNG AND I COPIED THE SERVER DRIVES. THE PROCESS OF COPYING THE SERVER DRIVES ALSO PROVED TO BE A LENGTHY PROCESS AS THE COPIES REQUIRED THE USE OF VMWARE SOFTWARE TO ENSURE A TRUE BIT FOR BIT COPY. AN ADDITIONAL COPY OF THE SERVERS WERE MADE IN THE EVENT THAT DRIVES SENT BY MAIL WOULD BE LOST. MY ADDITIONAL COPY WILL BE RETAINED UNTIL ALL DRIVES ARE RETURNED FROM MS-ISAC AND PLACED BACK INTO EVIDENCE AND AT THAT POINT THE DRIVE WILL BE REFORMATTED FOR ACSO. ALL DRIVES WILL REMAIN IN EVIDENCE UNTIL THIS CASE IS CLOSED.

08/14/2016:

INITIAL DISCUSION PERTAINING TO FINANCE AUDIT:

AFTER MEETING WITH BRIAN YOUNG, I DETERMINED THAT IT WOULD BE PRUDENT FOR AN AUDIT OF ANDERSON COUNTY FINANCES BE CONDUCTED TO DETERMINE IF FINANCES HAD BEEN TAMPERED WITH AS A RESULT OF ANY POSSIBLE UNAUTHORIZED ACCESS TO THE ANDERSON COUNTY SERVERS. I STRONGLY ADVISED MS. ERB THAT SHE NEEDED TO CONDUCT A FORENSIC AUDIT OF THE FINANCES OF THE COUNTY, STARTING WITH GOING INTO THE VAULT AND AUDITING ALL OF THE ORIGINAL CHECKS RECEIVED BACK FROM THE BANKS. I ADVISED MS. ERB THAT UNDER NO CIRCUMSTANCES DO I WANT ANY EMPLOYEE TO BE INTERVIEWED AS PART OF THE AUDIT. MS. ERB ASKED IF THE AUDIT REQUEST WAS SOMETHING THAT THE SHERIFF'S OFFICE WAS OFFICIALLY ORDERING AS PART OF THIS INVESTIGATION OR IS IT AN ISSUE FOR COUNTY COMMISSION. I ADVISED MS. ERB THAT, AT THIS POINT, IT IS UNKNOWN IF THE COUNTY HAD EVEN SUSTAINED AN UNAUTHORIZED ACCESS TO THE COUNTY'S SERVERS OR NETWORKS AND IF ANY DATA HAD BEEN ACCESSED AND/OR EX-FILTRATED. MS. ERB ADVISED THAT SHE WOULD HAVE TO TAKE THE ISSUE TO COUNTY COMMISSION DUE TO THE FACT THAT AN AUDIT WOULD HAVE TO BE PERFORMED BY AN EXTERNAL AGENCY. MS. ERB AGREED THAT THE SITUATION WARRANTED COUNTY COMMISSION BE ADVISED OF THE SITUATION. I INSTRUCTED MS. ERB THAT SHE IS NOT TO DIVULGE ANYTHING RELATING TO MY INVESTIGATION.

08/17/2016:

COMPUTER VIRUS INFECTED SERVER:

I WAS ADVISED BY BRIAN YOUNG THAT ANDERSON COUNTY GOVERNMENT WAS THE RECIPIENT OF A "CRYPTOLOCKER" TYPE VIRUS. THIS VIRUS' MAIN FUNCTION IS TO ENCRYPT ALL OF THE DATA THAT IS HELD ON A HARD DRIVE. THE DATA IS HELD "FOR RANSOM" AND A CODE IS GIVEN TO UNLOCK THE DATA ONCE IT IS PAID FOR BY THE VICTIM, USUALLY IN BITCOIN SO THAT THE TRANSACTION CANNOT BE TRACED. BRIAN YOUNG ADVISED THAT AS HE WAS CONDUCTING A BACKUP OF THE DATA ON THE SERVER, HE RECOGNIZED THE IMPLEMENTATION OF THE VIRUS AND ATTEMPTED TO STOP IT'S INTRODUCTION. BRIAN YOUNG ADVISED THAT THE CURRENT DATA ON THE SERVER IS NOW ENCRYPTED. I ASKED BRIAN YOUNG IF THIS VIRUS WAS A RESULT OF THE RECENT RELEASE OF THE NEWS STORY REPORTING THAT ANDERSON COUNTY SERVERS ARE VULNERABLE AND THAT UNAUTHORIZED INTRUSIONS OCCURRED. HE STATED THAT IT APPEARED TOO COINCIDENTAL THE TWO EVENTS OCCURRING SO CLOSE TOGETHER. I ADVISED BRIAN YOUNG THAT I HAD MADE AN EXTRA COPY OF THE IMAGING IN CASE OF LOSS DURING TRANSIT BACK AND FORTH BETWEEN ACSO AND MS-ISAC. I ADVISED THAT HE COULD USE THE COPY TO DELETE THE HARD DRIVE IN THE SERVER, REFORMAT AND MAKE A FRESH SERVER DRIVE SO THAT MINIMAL DATA LOSS WOULD OCCUR.

BRIAN YOUNG RETURNED THE DRIVE THAT WAS PROVIDED TO HIM AND ADVISED THAT BECAUSE OF THE EXTRA COPIED DRIVE, HE WAS ABLE TO RESTORE THE ANDERSON COUNTY GOVERNMENT SERVER WITH MINIMAL DATA LOSS. HE STATED THAT OTHERWISE, ALL OF THE DATA WOULD HAVE BEEN LOST WHICH WOULD HAVE SET ANDERSON COUNTY BACK NUMEROUS YEARS.

08/23/2016:

INITIAL EVIDENCE SENT TO MS-ISAC:

AFTER THE PROCESS OF COPYING THE DRIVES, I PROCEEDED TO FEDEX IN OAK RIDGE AND SENT THE ORIGINAL MIRRORED IMAGE AND LIVE MEMORY CAPTURE OF THE I.D. BADGE SERVER, THE THUMB DRIVE ORIGINALLY PROVIDED BY BRIAN YOUNG WHICH CONTAINS THE NTFS JOURNAL, THE DRIVE CONTAINING A TRUE IMAGE CAPTURE OF SERVERPDC, MAIL EXCHANGE SERVER EXCH2K10, AND A TOSHIBA USB EXTERNAL HARD DRIVE THAT WAS FOUND PLUGGED INTO THE FRONT FACE OF THE MAIN SERVER TO MS-ISAC IN NEW YORK.

I WAS ADVISED BY BRIAN YOUNG THAT HE HAD LOCATED ADDITIONAL BACK-UP SERVERS IN THE SERVER ROOM. IT WAS UNCLEAR AS TO IF THE SERVERS WERE USED ONLY AS BACK-UPS TO THE MAIN SERVER SYSTEM OR IF THEY WERE ACTIVELY COMMUNICATING WITH THE NETWORK. I INSTRUCTED BRIAN YOUNG TO SEIZE BOTH SERVER UNITS AND PLACE THEM IN A SECURED LOCATION THAT ONLY HE HAS ACCESS TO. I LATER TOOK POSSESSION OF BOTH SERVER UNITS AND PLACED THEM IN EVIDENCE.

AT THIS POINT, SINCE THE PRIORITY WAS TO GET THE MIRRORED IMAGES AND COPIED DRIVES SENT OFF TO MS-ISAC, WHICH WAS COMPLETED, I WAS ABLE TO FOCUS ON MEETING WITH BRIAN YOUNG AND FORMULATE A STRATEGY FOR

THE CONTINUED INVESTIGATION. ALSO, IN LIGHT OF THE FACT THAT IT WAS REPORTED THAT TWO PERSONS HAD REPORTED THAT THEIR CREDIT UNION ACCOUNTS HAD BEEN COMPROMISED, AND THE FACT THAT IDENTITY THEFT AND FRAUD MAY NOT BE EVIDENT FOR MONTHS, I SHALL BE KEEPING THIS REPORT OPEN, AND CONDUCT A MONTHLY SEARCH THROUGH ACSO REPORTS OF FRAUD AND IDENTITY THEFT, IN AN EFFORT TO DETERMINE IF THERE ARE CONNECTED INCIDENTS TO THIS INVESTIGATION. I WILL BE KEEPING THIS REPORT OPEN FOR A PERIOD OF 12 TO 18 MONTHS OR UNTIL I FIND NO RESIDUAL EVIDENCE OF AN UNAUTHORIZED ACCESS EVENT TO THE ANDERSON COUNTY SERVERS.

DURING THE COURSE OF MY INVESTIGATION, I FOUND THAT THE SERVER ROOM HAS NO SECURITY PROTOCOLS IN PLACE, OTHER THAN A SINGLE DOOR LOCK. THERE IS NO METHOD OF TRACKING WHO HAS ACCESSED THE ROOM AS WELL AS, MORE THAN ONE PERSON CAN ACCESS THE ROOM. NO VIDEO CAMERAS WERE FOUND AS WELL. I FOUND THAT TO BE ALARMING AND STRONGLY SUGGESTED TO BRIAN YOUNG AND NATALIE ERB HOW IMPORTANT AND IMPERATIVE THAT A BADGE READER AS WELL AS VIDEO CAMERAS BE INSTALLED BOTH OUTSIDE THE DOOR OF THE SERVER ROOM AND INSIDE TO MONITOR ACCESS.

I ADVISED BRIAN YOUNG THAT IF HE IS HIRED ON AS A FULL-TIME EMPLOYEE OF THE COUNTY, HE AND ONLY HE SHOULD HAVE ACCESS TO THE SERVER ROOM. I ADVISED BRIAN THAT HE SHOULD CONSIDER THE SERVER ROOM TO BE A TWO-MAN RULE AREA, AT LEAST UNTIL A FINAL DETERMINATION IS MADE AS TO WHO WILL MAINTAIN CONTROL AND RESPONSIBILITY OF THE SERVER. I ALSO ADVISED BRIAN YOUNG AND MS. ERB THAT A SIGN-IN LOG SHOULD ALSO BE CONSIDERED. FINALLY, I ADVISED THAT THE SERVER ROOM DOOR LOCK NEEDS TO BE CHANGED AND STRICT ACCESS TO THE KEYS SHOULD BE A POLICY.

09/02/2016:

H.R. DIRECTOR RUSSELL BEARDEN'S TERMINAL/EMAIL ISSUES DISCOVERED:

I WAS ADVISED BY BRIAN YOUNG THAT HE FOUND, WHAT HE SUSPECTED TO BE, AN UNAUTHORIZED ACCESS TO RUSSELL BEARDEN'S COMPUTER USING THE CLIENT TEAMVIEWER. YOUNG ADVISED THAT THE PROGRAM THAT APPEARED TO BE AFFECTED WAS AN EMAIL CLIENT SOFTWARE NAMED OUTLOOK. I DECIDED TO PROCEED TO RUSSELL BEARDEN'S OFFICE WITH A VIDEO CAMERA AND HAVE BRIAN YOUNG EXPLAIN THE NATURE OF THE UNAUTHORIZED EVENT. DURING THE COURSE OF CONDUCTING THE INTERVIEW, YOUNG REPORTED THAT THE ADMINISTRATOR SETTINGS OF OUTLOOK APPEAR TO BE SET INCORRECTLY. DURING THE VIDEO, YOUNG DEMONSTRATED HOW THE ADMINISTRATOR IS ABLE TO VIEW ALL OF THE "INBOX", "DRAFTS", "SENT ITEMS", DELETED ITEMS", "SPAM", "JUNK E-MAIL", "OUTBOX", "RSS FEEDS". I ASKED WHO THE ADMINISTRATOR IS FOR OUTLOOK. BRIAN YOUNG WAS UNABLE TO POSITIVELY IDENTIFY WHO THE EMAIL ADMINISTRATOR WAS PREVIOUS TO THIS INVESTIGATION. THE DEMONSTRATION HAS SHOWN THAT THE ADMINISTRATOR HAS THE ABILITY TO VIEW, MARK AS UNREAD, AND POTENTIALLY SEND EMAILS WITHOUT THE ANDERSON COUNTY EMPLOYEES HAVING KNOWLEDGE OF SUCH ACTIONS. I RECOMMENDED TO BRIAN THAT HE WOULD NEED TO CORRECT THE ISSUE AS SOON AS POSSIBLE.

09/08/2016:

UNEXPLAINED SPLITTER TYPE DEVICE (ITEM #15, BARCODE #2321) FOUND:

BRIAN YOUNG CONTACTED ME VIA PHONE AND INFORMED ME THAT A DEVICE WAS FOUND, PLUGGED INTO ONE OF THE NUMBERED PATCH PANEL PORTS OF THE SERVERS. THE DEVICE APPEARED TO BE A SMALL ETHERNET SPLITTER, MALE SINGLE END WITH TWO FEMALE ENDS. THE SPLITTER WAS FOUND PLUGGED INTO SLOT MARKED #46, WHICH IS ASSIGNED TO CHANCERY COURT FRONT COUNTER. ONE FEMALE END WAS USED FOR THE CHANCERY COURT FRONT COUNTER, THE OTHER END CONTAINED AN ETHERNET WIRE THAT WAS PLUGGED INTO FINANCE/MAYOR/H.R. SWITCH AS A CLOSED LOOPIT IS UNKNOWN IF THE DEVICE HAS ANY LEGITIMATE FUNCTION TO THE SERVER. THE SPLITTER HAS NO MEANS OF TRANSMITTING DATA BY ITSELF AND SERVES ONLY TO ADD ADDITIONAL LINES TO A CERTAIN NUMBERED SLOT. BRIAN YOUNG ADVISED THAT AT THE TIME OF HIS EXAMINATION OF THE SERVER, THERE WERE SUFFICIENT OPEN PORTS AVAILABLE. *IT SHOULD BE NOTED THAT IT IS UNKNOWN IF THE DEVICE WAS EVER USED IN A MALICIOUS MANNER I WAS LATER MADE AWARE BY OTHER IT VENDORS THAT THE SPLITTER DEVICE SERVES AS ADDING ADDITIONAL COMPUTER USERS ON THE SAME ASSIGNED PORT.

09/13/2016:

ADDITIONAL UNAUTHORIZED ACCESS REPORTED:

IT WAS REPORTED BY GALLAHER & ASSOCIATES THAT IT WAS SUSPECTED THAT ANOTHER UNAUTHORIZED ACCESS TO THE BADGE SERVER HAD OCCURRED. DUE TO ME BEING OUT OF THE AREA AT THE TIME OF THIS REPORTED EVENT, A MEETING WAS HELD BY SGT. DAVIS AND CPL. JAMES CROWLEY ALONG WITH ANDERSON COUNTY EMPLOYEES AND BRIAN YOUNG AS WELL AS GALLAHER & ASSOCIATES, WHO WAS ASKED TO GIVE THEIR SUSPICIONS AS TO WHAT HAPPENED. IT WAS ADVISED THAT ON 08/25/2016 AT 1257 HRS. THE BADGE SERVER WAS ACCESSED. DURING THAT ACCESS THERE WERE THREE ATTEMPTS BY THE QUICKTAG PROGRAM TO OPEN/ACCEESS THE SERVER USING WHAT WAS BELIEVED TO BE A BACK DOOR ACCESS. GALLAHER & ASSOCIATES REPORTED THAT ACCESS TO THE SERVER ON PREVIOUS INCIDENTS WERE MADE THROUGH THE BADGE SYSTEM AND THAT IT WAS POSSIBLE THAT SOME ACCESS BADGES COULD HAVE BEEN COPIED. SGT. DAVIS RECEIVED INFORMATION THAT THE ORIGINAL LOGS THAT INDICATED THAT THERE WAS SOME TYPE OF UNAUTHORIZED ACCESS, PREVIOUSLY, WERE GONE AND THAT SOMEONE HAD ENTERED THE SYSTEM AND CHANGED/REMOVED THE DATA. NO OTHER INFORMATION WAS OBTAINED OTHER THAN WHAT WAS ALREADY COMMONLY KNOWN BY BRIAN YOUNG AND RUSSELL BEARDEN.

MONTH OF SEPTEMBER 2016 FRAUD/IDENTITY THEFT REPORTS:

I FOUND THREE REPORTS OF FRAUD. ONE CASE INVOLVED CREDIT CARD LOSS. ONE CASE INVOLVED TELEPHONE SCAM FOR MONEY. ONE CASE INVOLVED THEFT.

I FOUND TWO REPORTS OF IDENTITY THEFT. ONE CASE INVOLVED THE VICTIM RECEIVING A CHECK IN THE MAIL FOR MONEY. FOUND TO BE UNRELATED TO THIS INCIDENT. ONE CASE INVOLVED ACCOUNTS BEING OPENED IN VICTIM'S NAME AT SUNTRUST BANK. NO RELATION TO THIS CASE FOUND.

10/07/2016:

REPORT RESULTS FROM MS-ISAC:

I RECEIVED, VIA. EMAIL, THE OFFICIAL FORENSIC ANALYSIS REPORT FROM MS-ISAC. IN THE REPORT, BY AARON MILLER, CERT ANALYST, HE STATED THAT ALL OF THE ITEMS SUBMITTED WERE EXAMINED TO INCLUDE REGISTRY DATA, LOGMEIN AND TEAMVIEWER DATA, WINDOWS EVENT LOGGING, AND RECOVERED DELETED DATA. THE REPORT FINDINGS WERE AS FOLLOWS:

- MS-ISAC FOUND NO EVIDENCE OF ANY TYPE OF UNAUTHORIZED ACCESS TO THE AFOREMENTIONED SYSTEMS TO INCLUDE THE BADGE SERVER, MAIN ACG SERVER AND MAIL EXCHANGE.
- THE BADGE PC PRIMARY ACCOUNT "DEFAULT" WAS FOUND TO BE USING LOCAL AUTHENTIFICATION AND ALL EVENTS WITH SAID ACCOUNT WERE FOUND TO BE INTERACTIVE OR NETWORK TYPE LOGINS TO SHARED FOLDERS. NO MALICIOUS EVENTS WERE FOUND AROUND THE TIMELINE OF REPORTED EVENTS.
- INTERACTIVE LOGON EVENTS INDICATE CONSOLE LOGINS AND APPEAR TO CORRELATE TO PERIODS WHEN LEGITIMATE SYSTEM MAINTENANCE OPERATIONS WERE BEING PERFORMED.
- LOGMEIN LOGS FOR THE EXCHANGE SERVER, DOMAIN CONTROLLER AND BADGE PC SHOW ACCESSES FROM MAIL.COMSYSPLUS.COM NETWORK, WHICH IS USED BY AN IT SUPPORT VENDOR.
- BASED ON DNS RECORDS, ANY CONNECTIONS FROM UNIDENTIFIED HOSTS (LISTED IN REPORT) WERE LIKELY MADE BY INDIVIDUALS LEGITIMATELY AFFILIATED WITH ACG, AND MAY HAVE BEEN WORKING FROM HOME. DURING THOSE TIMES, NO EVIDENCE OF LOG TAMPERING WERE FOUND.
- TEAMVIEWER ACCESS LOGS WERE REVIEWED. MS-ISAC FOUND THAT LOGS DO NOT SHOW IP ADDRESSES FOR INITIATED CONNECTIONS, BUT INSTEAD SHOW UNIQUE DEVICE ID'S, AS WELL AS REGISTERED NAMES. ONLY TWO NAMES WERE FOUND. 06/07/2016 HECTOR CRUZ (GALLAHER & ASSOCIATES SUB-CONTRACTOR) AND MULTIPLE USES BY BRIAN YOUNG (DURING INITIAL INVESTIGATION).
- AUTHENTIFICATION FAILURES WERE FOUND IN THE SECURITY LOG OF THE ON THE EXCHANGE SERVER. THESE FAILURES WERE EXPLAINED AS SIMPLE ISSUES SUCH AS HOST OR DNS CONFIGURATION SETTINGS. THE AUTHENTICATION FAILURES DO NOT APPEAR TO BE MALICIOUS.

- THE TIMELINE (BRIAN YOUNG'S TIMELINE WHICH INITIATED PRIOR TO ACSO INVOLVEMENT) WAS REVIEWED BY MS-ISAC. THE TIMELINE REPORTED CONTAINED POTENTIAL SECURITY EVENTS. ONE SUCH SECURITY RELATED EVENT WERE THE GAPS THAT WERE FOUND IN THE WINDOWS (NTFS) EVENT LOGS. MS-ISAC REVIEWED THE LOGS AND ONLY ONE SIGNIFICANT GAP WAS FOUND TO HAVE OCCURRED BETWEEN 05/20/2016 AND 05/26/2016. THE REASON FOR THE GAP WAS DUE TO A WINDOWS 10 UPGRADE PROCESS WHICH STARTED ON 05/20/2016. THE UPGRADE PROCESS SAT AT THE "NEXT" SCREEN UNTIL 05/26/2016 DURING WHICH TIME MOST SERVICES WERE SHUT DOWN AND VERY LITTLE LOGGING OCCURRED.
- THE TIMELINE REPORTED BADGE PC EVENT LOGS WHICH SHOW "IMPERSONATION WITH GUEST ACCOUNT" BETWEEN 05/20/2016 TO 05/21/2016, DEFAULT USER REQUESTING RUNNING PROGRAMS ON THE SERVER "KILL STRIKES", WITH SUBSEQUENT INCREASE IN USE OF DEFAULT ACCOUNT IN LATE HOURS BETWEEN JUNE AND JULY OF 2016. MS-ISAC FOUND NO GUEST IMPERSONATIONS OR MALICIOUS PROGRAM EXECUTIONS.
- NTFS TRANSACTIONS SHOW (ACCORDING TO BRIAN YOUNG TIMELINE) "TIMES THE GAPS WHERE IN THE LOGS THAT THE SYSTEM WAS PUSHING FILES OF UNKNOWN NAME TO WHAT APPEARS AS AN OUTLOOK CLIENT WITH AN ID OF NUMBERS THAT IN MY OPINION COULD BE THE MICROSOFT ID AT VERY LOW LEVEL SHOWING THE IDENTITY, IF MICROSOFT WOULD OR COULD GIVE THAT DATA THEY MAY BE ABLE TO SHED LIGHT ON THIS NOT SURE". MS-ISAC FOUND THAT ENTRIES RELATED TO OUTLOOK IN THE PROVIDED NTFS TRANSACTION LOG WERE THE RESULT OF APPLICATION UPGRADESAND FILE PLACEMENTS BEING CARRIED OUT BY WINDOWS UPDATE PROCESS. THE NUMBERS ATTACHED TO THE PACKAGES WERE NOT ID'S BUT RATHER A COMBINATION OF UPDATE PACKAGE NUMBERS AND INSTALLATION STATUS CODES.
- IT IS REPORTED THAT THE APPLICATION LOG ON THE BADGE PC SHOWS LOGINS BETWEEN 0300 – 0500 ON JULY 16 2016. MS-ISAC EXAMINED THE LOG AND FOUND NO EVIDENCE OF INTERACTIVE USE OF THE BADGE SYSTEM IN THE APPLICATION LOG OR THE SECURITY LOG DURING THIS PERIOD. ENTRIED RELATED TO THE EXECUTION OF LOGMEIN AND LOCAL DATABASES WERE NOTED AND WERE FOUND TO BE RELATED TO NORMAL STARTUP PROCESSES WHICH OCCURRED AS A RESULT OF THE SYSTEM BEING REBOOTED. THE REBOOT WAS A RESULT OF THE WINDOWS UPDATE SYSTEM.
- IT WAS REPORTED THAT THE APPLICATION LOG ON THE DOMAIN CONTROLLER WAS CLEARED ON 07/28/2016. MS-ISAC FOUND THAT THE APPLICATION LOG DOES NOT EXTEND VERY FAR BACK AND THE REASON FOR THIS IS DUE TO THE HIGH FREQUENCY OF ERRORS WHICH SPAN A SHORT TIMEFRAME BUT STILL CONSUMES THE MAJORITY OF SPACE RESERVED FOR LOG STORAGE. MS-ISAC FOUND NO EVIDENCE IN THE SECURITY LOG SUPPORTING MANUAL CLEAR OF THE APPLICATION LOG.
- IT WAS REPORTED IN THE TIMELINE "FOUND 2 WORKSTATIONS THAT WERE SHOWING AS CONNECTED IN THE RECENT ADDRESS LINE TO THE BADGE PC FROM THE WINDOWS EXPLORER ADDRESS BAR DROP DOWN WITH NO TIME STAMP IN THIS PROGRAM. THESE ID'S DISPLAYED WS-13717 & WS14173". MS-ISAC DID NOT HAVE DIRECT ACCESS TO THE ACTUAL WORKSTATION HOWEVER, THE BADGE PC DOES HAVE FILE SHARES ON IT, WHICH MAY SUPPORT A BUSINESS USE OF THE CONNECTIONS. MS-ISAC DETERMINED THAT THE PATHS WERE LIKELY ENTERED PRIOR TO 05/26/2016.
- ADDITIONALLY REPORTED TO MS-ISAC THE FOLLOWING, "ON A SECOND MATTER THE EXCHANGE SERVER YOU WILL BE VIEWING I HAVE FOUND INTERESTING SETUP WITH ADMIN PERMISSION ON FULL CONTROL WITH VARIOUS USERS (VISIBLE DELETED SID ACCOUNTS STILL EXIST? AS FULL PERMISSIONS CONTROL) IN THE EXCHANGE MANAGEMENT PANEL FULL PERMISSIONS. YOU WILL SEE SOME USERS HAD BUILT-IN ADMINISTRATORS AT FULL PERMISSIONS ON THEIR MAILBOXES. MS-ISAC MADE THE FOLLOWING DETERMINATION: BY DEFAULT, THE EXCHANGE ORGANIZATION ADMINISTRATORS GROUP IS GRANTED FULL CONTROL OVER THE EXCHANGE. THIS GROUP NORMALLY INCLUDES BUILT-IN ADMINISTRATOR ACCOUNT. IT IS LIKELY THAT ACCOUNTS WITH PERMISSIONS GRANTED TO THIS USER EXISTED DURING INITIAL SETUP OR

MIGRATION OF EXCHANGE. THE APPEARANCE OF SID'S IN THE PERMISSION LIST IS SOMEWHAT COMMON IN SITUATIONS WHERE THERE HAS BEEN A HIGH FREQUENCY OF STAFFING CHANGES.

- IT WAS REPORTED THAT "ACTIVE DIRECTORY USERS "RDP" AND "THMS" THESE 2 USERS HAD "ADMIN" LEVEL CONTROL AT LOGIN" MS-ISAC FOUND NO EVIDENCE THAT THE TWO ACCOUNTS WERE USED FOR REMOTE ACCESS.

RE-EVALUATION OF INVESTIGATION:

AFTER RECEIVING THE FORENSIC ANALYSIS REPORT AND REVIEWING IT'S CONTENTS, I ADVISED SGT. DAVIS OF THE FINDINGS IN THE REPORT. AT THIS POINT IN THE INVESTIGATION, THERE WAS NO EVIDENCE TO SUGGEST THAT AN UNAUTHORIZED ACCESS TO ANDERSON COUNTY GOVERNMENT SERVERS HAD OCCURRED. THE REPORT CONTRADICTED THE ORIGINAL COMPLAINT MADE BY H.R. DIRECTOR RUSSELL BEARDEN. I ADVISED SGT. DAVIS THAT THE FIREWALL THAT WAS IN PLACE AT THE TIME COULD NOT PROVIDE DATA TO ASSIST IN THIS INVESTIGATION. DURING OUR MEETING, I ALSO PRESENTED WHAT WINDSTREAM'S LEGAL DEPARTMENT HAD ADVISED CONCERNING THE ISSUE OF NOT MAINTAINING RECORDS OR A DATABASE OF I.P. ADDRESSES.

OTHER ISSUES THAT WERE PRESENTED IN THE MEETING INVOLVED "LOGMEIN" AND "TEAMVIEWER", BOTH REMOTE ACCESS PROGRAMS. AT THE TIME, LEADING UP TO AND SUBSEQUENT TO THE INITIAL PHASE OF THIS INVESTIGATION, THE USERNAME AND PASSWORDS FOR BOTH REMOTE ACCESS PROGRAMS AS WELL AS THE MAIN USERNAME AND PASSWORD FOR THE SERVERS WERE EXTREMELY SIMPLISTIC, WERE KNOWN BY NUMEROUS INDIVIDUALS, AND ALLOWED FULL ACCESS TO THE NETWORK. THE MAIN ISSUES THAT HINDER THIS INVESTIGATION, AS DISCUSSED WITH BRIAN YOUNG ARE AS FOLLOWS:

1. MS-ISAC REPORT CONTRADICTS INITIAL REPORT. NOTHING OF EVIDENTIARY VALUE OBTAINED FROM THE SUBMITTED EVIDENCE.
2. FIREWALL THAT WAS IN PLACE OVERWRITES DATA AND WAS SHOWN TO BE INADEQUATE FOR ANDERSON COUNTY GOVERNMENT NEEDS. THE FIREWALL PROVIDED NO DATA TO ASSIST MY INVESTIGATION.
3. USER ACCOUNT AND EMAIL ACCOUNT USERNAME AND PASSWORDS WERE WIDELY KNOWN BY OTHER EMPLOYEES. EMPLOYEES HAD THE ABILITY TO ACCESS OTHER EMPLOYEE EMAILS (NO INSTANCES REPORTED) DUE TO THE SIMPLISTIC USERNAMES AND PASSWORDS.
4. AT LEAST ONE EMPLOYEE HAD THE PASSWORD TO THE MAIN NETWORK SERVER.
5. TERMED OR INACTIVE EMPLOYEES ACCOUNTS STILL ACTIVE IN THE SYSTEM.

I ADVISED SGT. DAVIS THAT IT APPEARED THAT THERE WERE SEVERAL ISSUES INVOLVING THE DAILY UPKEEP OF ANDERSON COUNTY GOVERNMENT'S NETWORK TO INCLUDE EMAIL, SOFTWARE, COMPUTER PROBLEMS AND MANY OF OTHER PROBLEMS. THE MAIN REASON FOR THESE ISSUES APPEARED TO BE DUE TO THE FACT THAT THERE WAS NO KNOWLEDGEABLE POINT OF CONTACT BETWEEN VENDORS AND ANDERSON COUNTY GOVERNMENT AS WELL AS DAY TO DAY UPKEEP WHICH WAS VIRTUALLY NON-EXISTENT.
OUR DISCUSSION ALSO INVOLVED CONTACTING THE TBI POLYGRAPH EXAMINER AND HAVE TBI PLACE EMPLOYEES ON THE POLYGRAPH. THE MAIN ISSUE WITH CONDUCTING THIS TYPE OF MASS INTERVIEWING OR INTERROGATION IS SIMPLY, THERE IS NO EVIDENCE AT THIS POINT TO INDICATE THAT UNAUTHORIZED ACCESS TO ANDERSON COUNTY GOVERNMENT SERVERS HAD OCCURRED AND BRINGING EMPLOYEES IN FOR INTERVIEWS WOULD YIELD LITTLE TO NO RESULTS AND QUESTIONING WOULD BE EXTREMELY LIMITED.

FINALLY, I ADVISED SGT. DAVIS THAT I DID HAVE OTHER EVIDENCE THAT WOULD NEED TO BE SENT TO MS-ISAC AND AFTER RESULTS FROM THE FORENSIC ANALYSIS OF THOSE ITEMS ARE RECEIVED, WE COULD, AGAIN, RE-EVALUATE OUR POSITION IN THIS INVESTIGATION.
SGT. DAVIS CONCURRED WITH MY FINDINGS AND ADVISED ME TO CONTINUE UNTIL COMPLETION.

MONTH OF OCTOBER 2016 FRAUD/IDENTITY THEFT REPORTS:
I FOUND NO REPORTS OF IDENTITY THEFT AND THREE REPORTS OF FRAUD. ONE CASE INVOLVED A KNOWN FAMILY RELATIVE, NO RELATION TO THIS INCIDENT. ONE INVOLVES A BAD CHECK BEING WRITTEN. ONE CASE INVOLVES THEFT OF A CREDIT CARD.

11/15/2016:
RECOVERY OF H.R. BADGE COMPUTER:
I WAS CONTACTED BY BRIAN YOUNG AND WAS ADVISED THAT HE HAD RECOVERED A "LENOVO" COMPUTER(ITEM #16, BARCODE #2322) THAT WAS ORIGINALLY IN THE FRONT LOBBY AREA OF THE HUMAN RESOURCES OFFICE. BRIAN YOUNG ADVISED THAT THE COMPUTER WAS USED AS THE I.D. BADGE ACCESS FOR ALL COUNTY EMPLOYEES. I MET WITH BRIAN YOUNG AND TOOK POSSESSION OF THE COMPUTER AS WELL AS A "KINGSTON" 120GB SSD (ITEM #17, BARCODE #2323) BOTH ITEMS WERE ENTERED INTO EVIDENCE.

11/16/2016:
INTERNAL EXAMINATION OF H.R. COMPUTER:
BRIAN YOUNG AND MYSELF OPENED THE H.R. COMPUTER AND FOUND THAT IT CONTAINED A SINGLE WESTERN DIGITAL 500GB HARD DRIVE (ITEM #25, BARCODE #2331).THE DRIVE WAS REMOVED FROM THE COMPUTER AND PLACED IN EVIDENCE, PENDING COPYING.

DURING PREVIOUS INTERNAL EXAMINATIONS OF THE BACK-UP SERVERS AND OF THE H.R. COMPUTER, IT WAS LEARNED THAT I WOULD NEED A TOTAL OF FIVE LARGE CAPACITY HARD DRIVES TO COMPLETE THE IMAGING/COPYING PROCESS.

PURCHASE OF ADDITIONAL HARD DRIVES FOR IMAGING HARD DRIVES:
I PROCEEDED TO SHIELD'S ELECTRONIC SUPPLY AND PURCHASED FIVE ADDITIONAL HARD DRIVES FOR THE PURPOSE OF OBTAINING TRUE IMAGES OF THE BACK UP SERVERS ("SUPERMICRO" AND "AND CO") AND THE H.R. "LENOVO" COMPUTER

11/18/2016:
FWD. EMAIL FROM NATALIE ERB CONCERNING A POSSIBLE IDENTITY THEFT REPORT:
I RECEIVED A FWD. EMAIL FROM MS. ERB THAT WAS ORIGINALLY SENT TO RUSSELL BEARDEN CONCERNING A REPORT OF A FEMALE HAVING HER IDENTITY STOLEN. THE INDIVIDUAL, A CUSTOMER OF REGIONS BANK HAD REPORTED THAT SOMEONE, USING HER IDENTITY, HAD MADE PURCHASES IN ARKANSAS, CHATTANOOGA AND DALLAS WITHOUT HER KNOWLEDGE. THE VICTIM HAD PREVIOUSLY USED ANDERSON COUNTY GOVERNMENT SERVICES FOR PROPERTY TAX PAYMENTS, CAR REGISTRATION ISSUANCES/PAYMENTS AS WELL AS PASSPORT. MS. ERB ADVISED RUSSELL BEARDEN TO CONTACT THE VICTIM FOR FOLLOW-UP.

I CONDUCTED A SEARCH FOR IDENTITY THEFTS AND FRAUDS WHICH LISTED THE VICTIM'S NAME AND AFTER LOOKING THROUGH REPORTS, I COULD NOT FIND A COMPLAINT FROM THE VICTIM REPORTING IDENTITY THEFT. I DID, HOWEVER HAVE A MEETING WITH BRIAN YOUNG ABOUT THE ANDERSON COUNTY CLERK CONDUCTING BUSINESS ON THE SERVER. BRAIN YOUNG ADVISED THAT THE CLERK'S OFFICE HAS A SEPARATE SERVER AND HE DID NOT BELIEVE THAT THE SERVERS WERE CONNECTED. DUE TO THIS BEING A ISOLATED INCIDENT AND THAT THERE WAS NO EVIDENCE TO INDICATE THAT ANDERSON COUNTY SERVERS HAD SUSTAINED ANY UNAUTHORIZED ACCESS, I WILL MONITOR THIS INCIDENT FOR FUTURE ACSO REPORTS.

11/29/2016:

FORMATTING ADDITIONAL DRIVES FOR COPYING:

DUE TO THE LARGE SIZE OF THE DRIVES, FORMATTING TOOK LONGER THAN 24 HOURS. THESE DRIVES WERE VERY PROBLEMATIC AS ACSO EQUIPMENT WAS NOT SUITABLE FOR CONDUCTING THIS PROCESS. EVERY TIME I TRIED TO PERFORM THE FORENSIC FORMAT OF THE DRIVE, THE PROCESS WOULD STOP WITH ERRORS INVOLVED. THIS PROCESS WOULD EVENTUALLY RUN WELL INTO DECEMBER 2016 AS BRIAN YOUNG AND I TRIED SEVERAL TIMES TO COMPLETE THIS PROCESS. WE LATER LEARNED THAT THE ISSUE WAS WITH WINDOWS OPERATING SYSTEM RECOGNIZING THE FULL DRIVE CAPACITY. IT WOULD NOT BE UNTIL 12/27/2016 THAT THE FORMATTING PROCESS WOULD BE COMPLETED PROPERLY.

MONTH OF NOVEMBER 2016 FRAUD/IDENTITY THEFT REPORTS:

NO REPORTS OF FRAUD REPORTED. NO REPORTS OF IDENTITY THEFT REPORTED.

12/27/2016:

FORMATTING PROCESS COMPLETED:

EXPERIENCING REPEATED ISSUES WITH FORMATTING THE NEWLY PURCHASED DRIVES, I WAS ABLE TO COMPLETE THE PROCESS. I SENT AN EMAIL TO MS-ISAC ANALYST MIKE RICHIE AND ADVISED HIM THAT THE FORMATTING PROCESS WAS COMPLETED. I REQUESTED ADDITIONAL INFORMATION OF MS-ISAC REQUIREMENTS FOR COPYING THE SERVER AND H.R. COMPUTER DRIVES.

MONTH OF DECEMBER 2016 FRAUD/IDENTITY THEFT REPORTS:

NO REPORTS OF FRAUD REPORTED. NO REPORTS OF IDENTITY THEFT REPORTED.

01/03/2017:

RESPONSE FROM MS-ISAC:

I RECEIVED AN EMAIL FROM ANALYST MIKE RICHIE. HE ADVISED ME THAT THE PROCESS FOR COPYING THE DRIVES CONSISTS OF USING SOFTWARE (FTK IMAGER LITE) AS SPECIFIED IN THE IMAGING GUIDE PREVIOUSLY PROVIDED BY MS-ISAC. I WAS ADVISED TO ALSO USE A WRITE BLOCKER IN THE PROCESS. I DECIDED TO CONTACT THE F.B.I. CYBER-DIVISION AND REQUEST ASSISTANCE WITH THIS PROCESS DUE TO EXPERIENCING FORMATTING ISSUES.

I CALLED FBI AGENT LARA AND REQUESTED HIS ASSISTANCE WITH PERFORMING THE IMAGING/COPYING. HE ADVISED ME TO SEND A REQUEST TO HIM AND SENIOR AGENT DAN DAMRON AND PROVIDED ME THE PROPER EMAILING.

01/05/2017:

EMAIL REQUEST FOR ASSISTANCE SENT TO F.B.I.:

I SENT A FORMAL EMAIL REQUEST TO AGENT LARA AND SENIOR AGENT DAN DAMRON ADVISING BOTH OF WHAT EVIDENCE I HAD AND REQUESTING THEIR ASSISTANCE IN IMAGING THE DRIVES.

01/09/2017:

INITIAL RESPONSE FROM F.B.I.:

RECEIVED AN EMAIL RESPONSE FROM SENIOR AGENT DAN DAMRON. HE ADVISED THAT HE PASSED MY REQUEST ON TO HIS SUPERVISOR AND IS AWAITING AN APPROVAL FOR ASSISTANCE.

01/10/2017:

APPROVAL FOR F.B.I. ASSISTANCE:

I RECEIVED AN EMAIL APPROVAL FROM F.B.I. SENIOR AGENT DAN DAMRON. I CONTACTED HIM VIA. PHONE AND SET UP A DELIVERY DATE OF 01/12/2017.

01/12/2017:

RELEASE OF HARD DRIVES TO F.B.I. FOR COPYING:

I PROCEEDED TO F.B.I. CYBER-DIVISION IN KNOXVILLE AND MET WITH AGENT DAN DAMRON. I SIGNED OVER CUSTODY OF THE BELOW LISTED ITEMS TO HIS POSSESSION:

HARD DRIVE, 3TB(ITEM #23, BARCODE #2329) REMOVED FROM "SUPERMICRO" B/U SERVER
HARD DRIVE, 1TB(ITEM #24, BARCODE #2330) REMOVED FROM "SUPERMICRO" B/U SERVER
HARD DRIVE, 500GB,(ITEM #25, BARCODE #2331) REMOVED FROM BADGE COMPUTER
HARD DRIVE, 250GB(ITEM #26, BARCODE #2332) REMOVED FROM B/U SERVER
HARD DRIVE,2TB(ITEM #27, BARCODE #2333) REMOVED FROM B/U SERVER
HARD DRIVE, 3TB(ITEM #18, BARCODE #2324) NEW FORMATTED
HARD DRIVE, 1TB(ITEM #19, BARCODE #2325) NEW FORMATTED
HARD DRIVE, 1TB(ITEM #20, BARCODE #2326) NEW FORMATTED
HARD DRIVE, 1TB(ITEM #21, BARCODE #2327) NEW FORMATTED
HARD DRIVE, 2TB(ITEM #22, BARCODE #2328) NEW FORMATTED

01/19/2017:

ORIGINAL SET OF EVIDENCE SENT BACK FROM MS-ISAC:

I RECEIVED AN EMAIL FROM CERT ANALYST VALECIA STOCCHETTI, ADVISING THAT THE FIRST SET OF DRIVES AND THUMB DRIVE HAS BEEN SENT OUT FROM THEIR LOCATION. I WAS GIVEN A USPS TRACKING NUMBER OF 9405 8036 9930 0388 8551 48.

MONTH OF JANUARY 2017 FRAUD/IDENTITY THEFT REPORTS:

I FOUND THREE REPORTS OF FRAUD. ONE CASE INVOLVED USE OF A DEBIT CARD. ONE CASE INVOLVED COUNTERFEIT MONEY. ONE CASE INVOLVED FRAUDULENT USE OF DEBIT CARD FROM REGIONS BANK. ALL THREE CASES WERE FOUND TO BE UNRELATED TO THIS INCIDENT. I FOUND FOUR REPORTS OF IDENTITY THEFT. ONE INVOLVED UNKNOWN PERSONS OPENING UP A CREDIT CARD IN VICTIM'S NAME AND AN UNAUTHORIZED ADDRESS CHANGE FROM AN ITEM ORDERED THROUGH MAIL. ONE REPORT INVOLVED AN INDIVIDUAL OPENING A COMCAST CABLE ACCOUNT IN THE VICTIM'S NAME. ONE CASE INVOLVED THEFT FROM VICTIM'S WALLET AND BURGLARY TO SHED. ONE CASE INVOLVED AN INDIVIDUAL APPLYING FOR UNEMPLOYMENT BENEFITS IN THE VICTIM'S NAME. ALL INCIDENTS DID NOT APPEAR TO BE RELATED TO THIS CASE.

02/01/2017:

MEETING WITH TBI POLYGRAPH EXAMINER:

I MET WITH SPECIAL TBI AGENT C. KENDALL BARHAM FOR THE PURPOSE OF OBTAINING INFORMATION ON SETTING UP POLYGRAPH EXAMINATIONS FOR COUNTY EMPLOYEES AND WHAT WOULD BE NEEDED TO SET UP POLYGRAPH EXAMINATIONS IF THERE IS EVIDENCE OF UNAUTHORIZED ACCESS TO THE COUNTY SERVERS. I QUESTIONED AGENT BARHAM ABOUT LEGAL ISSUES OF POLYGRAPHING EMPLOYEES. HE ADVISED THAT HE WOULD RESEARCH THE SUBJECT AND WOULD GET BACK TO ME.

02/02/2017:

RESPONSE FROM TBI POLYGRAPH EXAMINER:

I RECEIVED AN EMAIL FROM SPECIAL AGENT BARHAM. IN HIS EMAIL HE COVERED TBI POLICY ON POLYGRAPH EXAMINATIONS AND THE BELOW LISTED STATEMENT:

"AS IT RELATES TO INTERNAL INVESTIGATIONS, T.B.I. POLICY 8-6-003 (H) (1) INDICATES THAT T.B.I. WILL ONLY CONDUCT POLYGRAPH EXAMINATIONS FOR LOCAL AGENCIES IF THE INTERNAL INVESTIGATION IS CRIMINAL IN NATURE. IT ALSO STATES THAT THE LOCAL AGENCY MUST BE WILLING TO PROSECUTE THE ALLEGED OFFENSE IF SUFFICIENT EVIDENCE IS DEVELOPED TO PROSECUTE THE SUSPECT. HOWEVER, THAT SAME POLICY STATES (AND I HAD FORGOTTEN) THAT T.B.I. WILL CONDUCT A POLYGRAPH EXAMINATION FOR A LOCAL AGENCY'S INTERNAL INVESTIGATION UPON THE WRITTEN REQUEST OF THE DISTRICT ATTORNEY GENERAL. SO, IF YOU REACH THE POINT IN THE INVESTIGATION THAT YOU DESIRE FOR AN EMPLOYEE TO SUBMIT TO THE POLYGRAPH EXAMINATION AND IT IS NOT CRIMINAL IN NATURE, T.B.I. WILL CONDUCT THAT EXAMINATION UPON RECEIVING A WRITTEN REQUEST FROM THE DISTRICT ATTORNEY GENERAL."

I PROCEEDED TO DISTRICT ATTORNEY GENERAL DAVE CLARK'S OFFICE AND MET WITH HIM ABOUT THE TBI POLICY OF POLYGRAPHING COUNTY EMPLOYEES AS RELATED TO CRIMINAL VS. INTERNAL INVESTIGATIONS. I ADVISED GENERAL CLARK THAT AS SOON AS I HAVE SOMETHING SUBSTANTIAL OR EVIDENCE THAT A CRIMINAL ACT HAD ACTUALLY OCCURRED, THEN MY PLAN WOULD BE TO MOVE INTO THE THIRD PHASE OF MY INVESTIGATION, INTERVIEWS. I ADVISED GENERAL CLARK THAT I DON'T HAVE EVIDENCE THAT WOULD SATISFY T.C.A. 39-14-602. GENERAL CLARK DID ADVISE THAT HE WOULD BE WILLING TO INITIATE A WRITTEN REQUEST TO TBI IF AND WHEN SAID REQUEST IS NEEDED.

02/03/2017:

EMAIL FROM F.B.I. AGENT DAN DAMRON:

I RECEIVED THE BELOW LISTED EMAIL FROM AGENT DAMRON. COMPLETION OF COPYING THE DRIVES WERE NOT DONE UNTIL 02/15/2017

"DET SCUGLIA,

JUST A QUICK UPDATE – WE ARE VERY CLOSE, I WOULD ANTICIPATE EARLY NEXT WEEK BUT ILL EMAIL YOU THEN. WE HAD SOME TROUBLE WITH THE 3TB HARD DRIVE WHILE IMAGING. IT WAS TAKING ABOUT A DAY TO DO AND THEN IT WOULD CRASH NEAR THE END. WE WERE ABLE TO USE ONE OF OUR 4TB HD'S AND IT FINALLY IMAGED SUCCESSFULLY. I DON'T THINK THERE WAS ANYTHING WRONG WITH YOUR 3TB HD, IT IS LIKELY THAT DUE TO SLIGHTLY DIFFERENT SIZES THERE JUST WASN'T ENOUGH ROOM. BUT ANYWAY, WE DID GET IT AND YOU GUYS CAN JUST HAVE THE 4TB HD. HOPE ALL IS WELL AND I'LL BE IN TOUCH EARLY NEXT WEEK.

THANKS,

DAN

02/16/2017:

RETREIVAL OF HARD DRIVES FROM F.B.I.:

I MET WITH SENIOR AGENT DAN DAMRON OF F.B.I. CYBER-DIVISION IN KNOXVILLE. HE ADVISED ME THAT THERE WERE SOME ISSUES IN COPYING THE DRIVES, BUT AGENTS WERE ABLE TO WORK THROUGH THE PROBLEMS AND WERE ABLE TO MAKE TRUE FORENSIC IMAGES OF ALL OF THE PROVIDED HARD DRIVES. ALL DRIVES WERE ACCOUNTED FOR AND RECEIVED BY ME.

02/22/2017:

SUBMISSION OF SECOND SET OF EVIDENCE TO MS-ISAC:

I PACKAGED THE BELOW LISTED ITEMS AND PROCEEDED TO FEDEX IN OAK RIDGE FOR SHIPPING ITEMS TO THE MS-ISAC FACILITY IN NEW YORK STATE:

HARD DRIVE (ITEM #19) MIRRORED IMAGE OF BACK UP SERVER
HARD DRIVE (ITEM #20) MIRRORED IMAGE OF BADGE COMPUTER
HARD DRIVE (ITEM #21) MIRRORED IMAGE OF OLD B/U SERVER
HARD DRIVE (ITEM #22) MIRRORED IMAGE OF OLD B/U SERVER
HARD DRIVE (ITEM #29) MIRRORED IMAGE OF BACK UP SERVER

MONTH OF FEBRUARY 2017 FRAUD/IDENTITY THEFT REPORTS:

I FOUND THREE REPORTS OF FRAUD. ONE REPORT INVOLVED ONLINE PURCHASES BY VICTIM AND INFORMATION WAS OBRTAINED. ONE CASE INVOLVED PURCHASING ITEMS FROM AN ONLINE WEBSITE AND RECEIVED BILLS FROM OTHER WEBSITES. ONE CASE INVOLVED A LOAN BEING OPENED IN VICTIM'S NAME. I FOUND ONE REPORT OF IDENTITY THEFT WHERE A PERSON RECEIVED A CREDIT CARD THAT THEY DID NOT APPLY FOR. ALL OF THE REPORTED INCIDENTS DID NOT APPEAR TO BE INVOLVED WITH THIS CASE.

03/23/2017:

MS-ISAC ANALYSIS REPORT FROM SECOND SUBMITTED EVIDENCE:

I RECEIVED VIA. EMAIL THE SECOND FORENSIC ANALYSIS REPORT FROM MS-ISAC ANALYST AARON MILLER. MILLER STATED IN HIS REPORT THAT HE RECEIVED FIVE DISK IMAGES FROM ACSO. THE REPORT STATES THE FOLLOWING:

- THIRD PARTY SOFTWARE IDENTIFIED ON THE LENOVO WORKSTATION INNCLUDED AN INSTALLATION OF THE DOOR SECURITY MANAGEMENT APPLICATION AS WELL AS THE "LOGMEIN" AND "TEAMVIEWER" REMOTE ACCESS APPLICATIONS. ALL DRIVE DATA WAS EXAMINED AND NO EVIDENCE OF SUSPICIOUS ACTIVITY WAS FOUND IN THE DATA.
- THE BACK UP SERVER (LINUX UBUNTU) INCLUDED TWO PARTITIONS AND INCLUDED A BACKUP PRODUCT "CRASHPLAN"WHICH WAS CONFIGURED TO PERFORM BACKUPS OF ACCOUNTING AND HR SERVERS. NO EVIDENCE WAS FOUND THAT WOULD INDICATE THAT THE SYSTEM WAS ATTACKED OR COMPROMISED.
- THE WINDOWS B/U SERVER WAS FOUND TO BE RUNNING WINDOWS 7 O.S. AS WELL AS "STORAGECRAFT" IMAGE MANAGER BACKUP SOLUTION. LOGS WERE EXAMINED AND FOUND THAT THREE SERVERS WERE BEING BACKED UP TO THE SYSTEM, "EXCH2010", "SERVERLG" AND "SERVERPDC". "LOGMEIN" WAS ALSO FOUND ON IN THE LOGS AND WAS REVIEWED FOR POTENTIALLY UNAUTHORIZED ACTIVITY. ALL REMOTE ACCESS ACTIVITY WAS FOUND TO BE FROM EITHER LOCAL ANDERSON COUNTY ADDRESSES OR PREVIOUSLY IDENTIFIED I.T. CONTRACTORS. NO EVIDENCE OF SUSPICIOUS OR UNEXPLAINED ACTIVITY WAS IDENTIFIED ON THIS SYSTEM.

MONTH OF MARCH 2017 FRAUD/IDENTITY THEFT REPORTS:

I FOUND FIVE REPORTS OF FRAUD. ONE REPORT INVOLVED A LOST CREDIT CARD BEING USED. ONE REPORT INVOLVED A PERSON USING VICTIM'S INFORMATION TO OBTAIN A COMCAST ACCOUNT AT AN ADDRESS. ONE REPORT INVOLVED UNKNOWN PERSONS ATTEMPTING TO USE VICTIM'S DISCOVER CARD. ONE REPORT INVOLVED FRAUDULENT USE OF CREDIT CARD. ONE REPORT INVOLVED CHECK FRAUD.

I FOUND ONE REPORTED FRAUD CASE. THE CASE INVOLVED A LOAN BEING TAKEN OUT ON 01/2016 UNKNOWN TO VICTIM. ALL OF THE REPORTED INCIDENTS DID NOT APPEAR TO BE INVOLVED WITH THIS CASE.

04/03/2017:

FOLLOW-UP REQUEST TO MS-ISAC REGARDING FINAL REPORT:

I CONTACTED SENIOR CERT ANALYST BRADLEY MCALLISTER, SPECIFICALLY TO ASK IF MS-ISAC WOULD BE ABLE TO PROVIDE ME A LISTING OF LOGINS RELATED TO "LOGMEIN" TO INCLUDE DATES AND TIMES. HE ADVISED THAT HE WOULD PERFORM THE REQUESTED EXAMINATION AND PROVIDE ME A REPORT.

04/10/2017:

FINAL FORENSIC ANALYSIS REPORT FROM MS-ISAC REGARDING "LOGMEIN":

WHILE ALL LOGINS ASSOCIATED WITH THE LOGMEIN SERVICE ON THE HR SYSTEM WERE REQUESTED, THE LOGMEIN LOGS AVAILABLE ON THE SYSTEM DID NOT CONTAIN ANY LOGINS. THE ONLY COMMUNICATIONS CONTAINED WITHIN THE LOGMEIN LOGS WERE RELATED TO THE LOGMEIN SERVICE CHECKING IF A NEWER VERSION WAS AVAILABLE, THE REMOTE ANTI-VIRUS MONITORING FUNCTION FOR THE SOFTWARE WHICH REPORTS THE CURRENT STATUS OF THE ANTI-VIRUS SOLUTIONS ON THE SYSTEM, AND THE LOGMEIN SERVICE CONNECTING TO THE LOGMEIN[.]COM DOMAIN IN SUPPORT OF THESE OR SIMILAR ACTIVITIES. ADDITIONALLY, ANDERSON COUNTY REPORTED LOGMEIN ACTIVITY OCCURRING IN EARLY AUGUST 2016, BUT THE LOGMEIN LOGS ON THE SYSTEM END ON JULY 24, 2016. ANDERSON COUNTY ALSO REPORTED WHAT WAS TERMED "TRIPLE DEFRAG" ACTIVITY, BUT THE EXECUTIONS OF THE "DEFRAG.EXE" PROCESS, FROM THE AVAILABLE DATA, WERE BEING RUN AS PART OF STANDARD WINDOWS ACTIVITY OR AS A SCHEDULED TASK, WHICH IS ALSO DEFAULT FOR WINDOWS SYSTEMS.

WHILE THESE INCONSISTENCIES CANNOT BE EXPLAINED WITH THE DATA AVAILABLE, THE SYSTEM BEING ANALYZED CONTINUED TO BE USED UNTIL AT LEAST SEPTEMBER 13. THE ACTIVITY DURING THIS TIME INCLUDED THE UNINSTALLATION OF MULTIPLE APPLICATIONS TO INCLUDE LOGMEIN ON AUGUST 31, INSTALLATION AND EXECUTION OF NEW UTILITIES, SUCH AS SPYBOT SEARCH AND DESTROY ON SEPTEMBER 1, AND THE CREATION OF A NEW USER ACCOUNT NAMED "HR.HR-WORKSTATION" ON SEPTEMBER 1.

THIS CONTINUED ACTIVITY ON THE SYSTEM, AFTER THE DATE OF THE SUSPECT ACTIVITY, COULD HAVE RESULTED IN THE REMOVAL OR ALTERATION OF FORENSIC ARTIFACTS PERTINENT TO THE INVESTIGATION. WHEN AN INCIDENT OCCURS OR IS SUSPECTED, QUICKLY OBTAINING A FORENSIC IMAGE OF THE SYSTEM OR LIMITING ACTIVITY ON THE SYSTEM UNTIL ONE CAN BE ACQUIRED HELPS TO PRESERVE THE INTEGRITY OF THE AVAILABLE EVIDENCE, IF ANY.

FINAL EVALUATION OF INVESTIGATION TO DATE:

AFTER RECEIVING THE FINAL REPORT FROM MS-ISAC, I HAD ANOTHER MEETING WITH SGT. DAVIS AND ADVISED HIM THAT MS-ISAC HAD FOUND NO EVIDENCE ON ANY OF THE SERVER DRIVES AND HR COMPUTER AND SERVER THAT INDICATES THAT AN UNAUTHORIZED INTRUSION INTO THE NETWORK HAD OCCURRED. MS-ISAC HAD EXPLAINED ALL OF THE REPORTED SUSPICIOUS EVENTS AS NORMAL UPDATING OR REGULAR NETWORK PERFORMANCES. I ADVISED SGT. DAVIS THAT I FOUND NO EVIDENCE OF CRIMINAL BEHAVIOR IN THIS INVESTIGATION.

I ALSO ADVISED SGT. DAVIS THAT I WOULD BE CONTINUING THIS INVESTIGATION BY PERFORMING MONTHLY REPORT CHECKS OF FRAUD AND IDENTITY THEFT UNTIL SUCH TIME AS EITHER NEW INFORMATION IS PRESENTED OR NOTHING OF EVIDENTIARY VALUE IS LEARNED.

DURING THE COURSE OF OUR DISCUSSION, THE SUBJECT OF PERFORMING A FORENSIC AUDIT WAS BROUGHT UP. I ADVISED SGT. DAVIS THAT, AT THIS POINT, I FELT THAT COUNTY COMMISSION IS WAITING TO SEE IF THERE IS SOMETHING THAT WOULD WARRANT THE AUDIT. I ADVISED SGT. DAVIS THAT I WOULD NOT CLOSE THIS CASE UNTIL THE MONTHLY FOLLOW-UPS WERE COMPLETED.

MONTH OF APRIL 2017 FRAUD/IDENTITY THEFT REPORTS:

I FOUND THREE REPORTS OF FRAUD AND NO REPORTS OF IDENTITY THEFT. ONE CASE OF FRAUD INVOLVED PORNOGRAPHIC SCAM FOR MONEY. ONE CASE INVOLVED A HACKED EBAY ACCOUNT. ONE CASE INVOLVED A FRAUDULENT HOME DEPOT CREDIT CARD. NONE OF THE INCIDENTS APPEARED TO BE RELATED TO THIS INVESTIGATION.

MONTHLY CONSULTATION WITH BRIAN YOUNG:

I MET WITH BRIAN YOUNG ABOUT THIS INVESTIGATION AND DISCUSSED WITH HIM IF HE HAD EXPERIENCED RESIDUAL SECURITY ISSUES. HE ADVISED THAT HE HAS NOT HAD ANY ISSUES AND HAS NOTHING NEW TO REPORT.

MONTH OF MAY 2017 FRAUD/IDENTITY THEFT REPORTS:

I FOUND THREE REPORTS OF FRAUD AND THREE REPORTS OF IDENTITY THEFT. ONE FRAUD REPORT INVOLVED A KNOWN FEMALE SUSPECT. ONE FRAUD REPORT INVOLVED AN EX-WIFE POSSIBLY MAKING UNAUTHORIZED CHARGES ON ACCOUNT. ONE FRAUD REPORT INVOLVED STOLEN CASH AND CREDIT CARD, KNOWN SUSPECT. NONE OF THE FRAUD REPORTS APPEARED TO BE RELATED TO THIS INCIDENT. ONE IDENTITY THEFT REPORT INVOLVED AN UNEMPLOYMENT CLAIM AND A FRAUDULENT CREDIT CARD APPLICATION. ONE REPORT OF IDENTITY THEFT INVOLVED AN UNKNOWN MALE ATTEMPTING TO HAVE MONEY DEPOSITED INTO AN ACCOUNT AND PURPORTED HIMSELF TO BE THE INTENDED VICTIM. ALL OF THE IDENTITY THEFT REPORTS DID NOT APPEAR TO BE RELATED TO THIS INVESTIGATION.

MONTHLY CONSULTATION WITH BRIAN YOUNG:

I MET WITH BRIAN YOUNG ABOUT THIS INVESTIGATION AND TO DETERMINE IF THERE HAD BEEN ANY CONTINUED ISSUES WITH ACG NETWORK. HE ADVISED THAT THE NETWORK WAS RUNNIG WITHOUT ISSUES AND HAD NOTHING ELSE TO REPORT.

MONTH OF JUNE 2017 FRAUD/IDENTITY THEFT REPORTS:

I FOUND TWO FRAUD REPORTS AND ONE REPORT OF IDENTITY THEFT. ONE FRAUD REPORT INVOLVED MINOR CHARGES TO VICTIM'S ONLINE GAMING ACCOUNT. ONE FRAUD REPORT INVOLVED THE PURCHASE OF A DOG, PAYMENT WAS FRAUDULENT. THE IDENTITY THEFT REPORT INVOLVED A LOST SS CARD, DRIVER'S LICENSE. NONE OF THE INCIDENTS APPEARED TO BE RELATED TO THIS INVESTIGATION.

MONTHLY MEETING WITH BRIAN YOUNG:
I MET WITH BRIAN YOUNG IN REFERENCE TO THE CURRENT STATE OF ACG NETWORK AND IF HE WAS EXPERIENCING ANY PROBLEMS WITH THE SYSTEM. HE ADVISED THAT THE SYSTEM WAS RUNNING FINE, WITH NO ISSUES OTHER THAN MINOR, REGULAR USER RELATED ISSUES. HE ADVISED THAT WITH THE NEW SECURITY THAT HAS BEEN IN PLACE, HE HAS NOT HAD ANY PROBLEMS TO REPORT.

MONTH OF JULY 2017 FRAUD/IDENTITY THEFT REPORTS:
I FOUND TWO FRAUD REPORTS AND THREE IDENTITY THEFT REPORTS. ONE FRAUD REPORT INVOLVED VICTIM BEING COERCED INTO PAYING MONEY. ONE FRAUD REPORT INVOLVED CRAIGSLIST. ONE IDENTITY THEFT REPORT INVOLVED AN INCIDENT THAT OCCURRED IN MARCH OF 2016 AND DID NOT BECOME APPARENT UNTIL THIS MONTH. ONE IDENTITY THEFT INVOLVED UNKNOWN PERSON OPENING A VERIZON ACCOUNT IN THE VICTIM'S NAME. ONE REPORT OF IDENTITY THEFT INVOLVED UNKNOWN PERSON USING VICTIM'S SS NUMBER IN TEXAS. NONE OF THE REPORTED INCIDENTS APPEAR TO BE INVOLVED WITH THIS INVESTIGATION.

08/01/2017:
MEETING WITH STATE OF TENNESSEE COMPTROLLER OF THE TREASURY DEPT.:
AT APPROXIMATELY 1000 HRS. BRIAN YOUNG AND I MET WITH GREG BRUSH, MICHAEL JARREAU, MARK TREECE AND AMY SOSVILLE, OF THE STATE COMPTROLLER'S OFFICE. IT WAS MY INTENTION TO ADVISE THEM OF MY INVESTIGATION AND TO FORMULATE A PLAN TO EXECUITE AN AUDIT.

DURING THE MEETING, WE DISCUSSED OPTIONS FOR HOW TO PROCEED WITH A FORENSIC AUDIT OF THE ANDERSON COUNTY FINANCE OFFICE. THOSE OPTIONS ENTAILED COUNTY COMMISSION VOTING TO HAVE THE AUDIT DONE, WHICH WOULD HAVE TO BE DONE BY A STATE CERTIFIED AUDIT COMPANY. I WAS ADVISED THAT THE COST OF CONDUCTING THE AUDIT COULD COST THE COUNTY UP TO OR IN EXCESS OF ONE-HUNDRED THOUSAND DOLLARS.

I WAS ADVISED THAT THE COMPTROLLER'S OFFICE WOULD BE CONDUCTING THEIR NORMAL AUDIT OF ENTRIES IN "ZORTEC" AND COMPARE THEM WITH "IMAGE EAZE". I WAS ADVISED THAT THE COMPTROLLER'S OFFICE WOULD REPORT DIRECTLY TO ME IF THERE ARE ANY DISCREPENCIES OR ANY SUSPICIOUS ACTIVITY. I WAS ADVISED THAT THE COMPTROLLER AUDITOR WILL GO BACK TO 01/01/2016 TO JULY 2016.

I WAS ADVISED THAT I WOULD BE NOTIFIED AT THE COMPLETION OF THE AUDIT AND WOULD BE ADVISED OF ANY ISSUES OR FINDINGS RELATED TO THIS INVESTIGATION.

MONTH OF AUGUST 2017 FRAUD/IDENTITY THEFT REPORTS:
I FOUND SIX FRAUD REPORT AND NO IDENTITY THEFT REPORTS. ALL BUT TWO INVOLVED FRAUDULENT USE OF CREDIT CARDS OR CREDIT CARD NUMBERS BEING FRAUDULENTLY USED. ONE FRAUD REPORT INVOLVED THE VICTIM SENDING A LARGE AMOUNT OF MONEY TO AN UNKNOWN INDIVIDUAL IN NEW YORK. ONE FRAUD REPORT INVOLVED A BUSINESS TAKING A ROLL OF DIMES WHICH DID NOT HAVE MONEY INSIDE THE ROLL. NONE OF THESE REPORTED INCIDENTS APPEARED TO BE RELATED TO THIS INVESTIGATION.

MONTH OF SEPTEMBER 2017 FRAUD/IDENTITY THEFT REPORTS:
I CONDUCTED A SEARCH AND FOUND FOUR REPORTS OF FRAUD AND THREE REPORTS OF IDENTITY THEFT. IN SEARCHING EACH REPORT WHICH INVOLVED CREDIT CARD THEFT, FRAUDULENT PURCHASES, AND OPENED ACCOUNTS BY KNOWN RELATIVE, I FOUND NO APPARENT RELATION BETWEEN THE REPORTED INCIDENTS AND THIS INVESTIGATION.

MONTH OF OCTOBER 2017 FRAUD/IDENTITY THEFT REPORTS:
I CONDUCTED A SEARCH FOR FRAUD AND IDENTITY THEFT CASES. I FOUND FIVE FRAUD REPORTS AND THREE IDENTITY THEFT REPORTS. AFTER REVIEWING ALL OF THE REPORTED INCIDENTS WHICH INVOLVED CREDIT CARD PURCHASE AND FRAUDULENT BANK ACCOUNTS BEING OPENED. I FOUND ONE IDENTITY THEFT CASE WHICH INVOLVES AN ANDERSON COUNTY COMMISSIONER. ID COMMANDER, AN IDENTITY THEFT PROTECTION SERVICE FOR ANDERSON COUNTY GOVERNMENT EMPLOYEES, HAD EMAILED THE VICTIM AND ADVISED THAT THE VICTIM'S PHONE NUMBER MAY HAVE

BEEN USED ON SOMEONE ELSE'S ACCOUNT WITHOUT HIS PERMISSION. THE INVESTIGATION WAS CONDUCTED BY DET. JAMES CROWLEY. IT WAS DETERMINED THAT SOMEONE POSSIBLY ENTERED A WRONG PHONE NUMBER AND THAT THIS WAS INADVERTENT. ORIGINAL REPORT ATTACHED TO THIS INVESTIGATION FOR FOLLOW-UP IF NEEDED.

11/09/2017:

CONTACT WITH THE CONTRACTED I.T. VENDOR TECHNICIAN:

I WAS ABLE TO MAKE CONTACT WITH THE TECHNICIAN THAT HAD BEEN SERVICING THE I.T. NEEDS OF ANDERSON COUNTY GOVERNMENT. AFTER IDENTIFYING MYSELF ON THE PHONE, I REQUESTED A MEETING WITH HIM AND ADVISED HIM THAT I WAS EXAMINING SOME REPORTED ISSUES THAT I WOULD LIKE TO RESOLVE. I ASKED IF I COULD MEET WITH HIM TO DISCUSS THIS MATTER. THE TECHNICIAN REFUSED TO AGREE TO TALK WITH ME AND FURTHER ADVISED THAT HE WOULD ONLY TALK TO ME IF HE WAS ADVISED BY LEGAL COUNSEL OR THE C.E.O. OF THE COMPANY. I IMMEDIATELY ENDED THE CONVERSATION AND ELECTED TO CONTACT THE CONTRACTED I.T. VENDOR C.E.O.

11/10/2017:

CONTACT WITH THE CONTRACTED I.T. VENDOR C.E.O.:

I CONTACTED THE C.E.O. VIA PHONE AND EXPLAINED MY REASON FOR WAS CONTACTING HIM. I ADVISED HIM THAT ONE OF HIS TECHNICIANS HAD REFUSED TO SPEAK WITH ME AND ASKED IF HE COULD PERSUADE HIM TO DISCUSS THE MATTER. I WAS ADVISED THAT HE COULD NOT FORCE THE TECHNICIAN TO SPEAK WITH ME. HE ALSO ADVISED THAT HE, HIMSELF WOULD ONLY BE WILLING TO ANSWER PRE-WRITTEN QUESTIONS AND WOULD HAVE TO GET BACK TO ME AT A LATER TIME UPON COMPLETION. I AGREED TO HIS TERMS AS IT IS MY OPINION THAT SOME ANSWERS FROM THE CONTRACTED VENDOR WOULD BE BETTER THAN NO ANSWERS. I ADVISED HIM THAT I WOULD EMAIL HIM A LIST OF QUESTIONS.

I NOTIFIED BRIAN YOUNG THAT AS SOON AS HE HAS FREE TIME, PLEASE COME TO MY OFFICE TO ASSIST IN COMPILING A LIST OF QUESTIONS.

11/16/2017:

QUESTIONARE SENT TO CONTRACTED I.T. VENDOR FOR ANDERSON COUNTY:

I SENT AN EMAIL TO THE CONTRACTED I.T. VENDOR C.E.O. WHICH ALSO CONTAINED A LIST OF QUESTIONS. BELOW IS AN ABBREVIATED VERSION OF THE EMAIL. I HAVE REDACTED CERTAIN REFERENCES IN THE QUESTIONS FOR REASONS OF OBJECTIVITY.

I APPRECIATE YOU TAKING THE TIME TO SPEAK WITH ME REGARDING MY INVESTIGATION INTO THE REPORTED ANDERSON COUNTY SERVER BREACH. AS PER OUR CONVERSATION, I HAVE LISTED THE BELOW SET OF QUESTIONS THAT I WOULD LIKE ANSWERED. THE QUESTIONS WERE PREVIOUSLY COMPILED DURING THE COURSE OF MY INVESTIGATION AND SOME OF WHICH WERE SPECIFICALLY CREATED BY OUR IT DIRECTOR ONLY FOR THE PURPOSE OF EXPLAINING SOME ISSUES THAT WERE DISCOVERED. THANK YOU IN ADVANCE FOR TAKING TIME TO SPEAK WITH ME AND ANSWER THESE QUESTIONS.

1. WHO WAS PHYSICALLY INVOLVED IN SETTING UP THE ANDERSON COUNTY SERVER INFRASTRUCTURE, INCLUDING FIREWALL, TERMINALS, WIRING, BADGING TERMINAL AND WORKSTATIONS?

2. WERE YOU AWARE THAT THE BADGE SECURITY COMPUTER HAD INTERNET ACCESS AND IF SO, WHAT WAS THE PURPOSE OF INTERNET ACCESS VIA THIS COMPUTER?

3. WHY DID THE BADGE SECURITY COMPUTER HAVE A SIMPLE USERNAME SIGN-ON? USERNAME: SECURITY (ALL USING SAME PASSWORD)?

4. WHY WAS THERE AN OPEN PORT IN THE SERVER ROOM WHICH SETS THE INDIVIDUAL KEYS FOR EACH BADGE? (WHY WAS THE DEVICE'S PHYSICAL LOCATION IN THE SERVER ROOM?)

5. WHY WAS "LOGMEIN" REMOTE CONTROL INSTALLED ON THE BADGE SECURITY SERVER (IN SERVER ROOM) AND ON THE BADGE ACCESS COMPUTER TERMINAL (IN H.R. OFFICE)?

6. HOW MANY EMPLOYEES HAD KNOWLEDGE AND ACCESS TO THE "LOGMEIN" REMOTE CONTROL? (WHO WAS GIVEN THE PASSWORD, WHICH WAS LISTED AS "DEFAULT" AND NEVER CHANGED)

7. HOW OFTEN WERE THE BADGE SECURITY COMPUTER SYSTEM PASSWORD CHANGED/UPDATED? (FOUND TO STILL BE "DEFAULT" AT TIME OF INVESTIGATION)

8. WHY WAS THE FORMAT FOR EMPLOY PASSWORDS SET AS FIRST INITIAL, LAST NAME, YEAR OF HIRE? (EX. JDOE2017. MOST OF EVERYONE KNEW OTHER'S PASSWORDS)

9. WHY WAS THE BARACUDA FIREWALL CHOSEN AS THE FIREWALL FOR A.C. SERVER?

10. THE TRANSACTION LOGS FOR THE FIREWALL WERE FOUND TO BE LIMITED AND DATA WAS OVERWRITTEN LESS THAN EVERY 24 HOURS. WHY WERE THOSE PARTICULAR SETTINGS CHOSEN AS THE DEFAULT?

11. WHY WERE 5 VLANS BEING ROUTED THROUGH THE AFOREMENTIONED BARACUDA FIREWALL?

12. WHY WAS A CISCO ASA FIREWALL FOUND SETTING POWERED BUT UNUSED ALONGSIDE THE OTHER FIREWALL? THE CISICO WAS POWERED ON, BUT NOT CONNECTED TO ANYTHING?

13. NO LABELS WERE FOUND ON ANY PIECE OF WIRING WHICH IDENTIFIED EACH INDIVIDUAL CONNECTION FROM THE SERVER TO THE WORKSTATIONS. HOW WAS THE WIRING MAPPED AND MAINTAINED?

14. A CAT5 SPLITTER WAS FOUND INSTALLED IN THE SWITCHPORT OF THE SERVER. WHAT WAS THE PURPOSE OF USING THE SPLITTER WHEN THERE WERE OPEN PORTS AVAILABLE?

15. THE SPLITTER CONNECTED THE SWITCHPORT TO THE TNCIS (CHANCERY COURT FRONT COUNTER) TO THE FINANCE VLAN (CONNECTING A BRIDGE). WHY?

16. WHY WAS REMOTE DESKTOP USER GROUP GIVEN ADMINISTRATIVE CONTROL GROUP PRIVILEGES TO THE SERVERS?

17. ARE OR WERE YOU AWARE THAT ALL STAFF HAD REMOTE LOG IN PRIVILEGES TO THE A.C. SERVER?

18. IF SO, WERE THERE ANY ATTEMPTS MADE TO ADDRESS THAT POTENTIAL PROBLEM?

19. HOW OFTEN DID YOU ACCESS THE SERVER FOR MAINTENANCE?

20. WERE THERE BACKUPS BEING CONDUCTED AND IF SO, WHERE ARE THEY STORED (IF OFF-SITE)? WHO HAS/HAD ACCESS TO THE BACKUPS?

21. WHY WAS THE ROOM WITH THE ICEMAKER MACHINE (DIFFERENT AREA THAN FINANCE OFFICE) AND THE FINANCE ROOM (DOOR 212) SET TO THE SAME ACCESS? (ALL PERSONNEL HAD ACCESS TO THE ICEMAKER ROOM AND WAS ALSO ABLE TO ACCESS THE MAIN FINANCE OFFICE DUE TO THAT PROGRAMMED ACCESS. FYI, THE SERVER ROOM WHICH WAS NOT LOCKED WAS IN THE FINANCE OFFICE).

22. ARE THERE RECORDS FOR SERVER MAINTENANCE TO INCLUDE FIRMWARE AND SOFTWARE UPDATES?

23. WHAT WAS THE PROCESS FOR VIRUS SCANNING OF THE SERVER AND WORKSTATIONS?

24. WERE YOU AWARE THAT THERE WERE SEVERAL PC'S RUNNING WITH ACTIVE KEYLOGGING SOFTWARE?

25. IF SO, WHO IMPLEMENTED THE INSTALLATION OF THE KEYLOGGERS AND BY WHO'S AUTHORITY?

26. WHO INSTALLED AND MAINTAINED "LOGMEIN" ON A.C. SERVER AND WORKSTATIONS?

27. DID ANY EMPLOYEE ACCESS A.C. SERVER AND/OR WORKSTATIONS AFTER AUGUST 4TH 2016?

28. WHO ALL HAD ACCESS, TO THE A.C. SERVER VIA LOGMEIN?

29. WHO SET UP CHANCERY COURT COMPUTER SYSTEMS? WHY WAS THEIR DATA STORED LOCALLY IN "C" DRIVES ON EACH WORKSTATION AS OPPOSED TO THE ACTUAL SERVER STORAGE DRIVES?

30. A "CRYTO LOCK" VIRUS INFECTED A.C. SERVER IN FEBRUARY/MARCH OF 2016 AND AGAIN IN MAY OF 2016. WHAT STEPS WERE IMPLEMENTED TO PREVENT FUTURE INFECTIONS OF THIS TYPE OF VIRUS?

31. WHO SET UP THE A.C. EMAIL SERVER?

32. WHO WAS GIVEN ADMINISTRATOR RIGHTS FOR THE EMAIL SYSTEM?

33. WHY WAS THE EMAIL GROUP FOR A.C. TITLED "MY PEEPS"?

34. EMPLOYEES MADE REGULAR COMPLAINTS ABOUT THEIR EMAILS BEING COMPROMISED BY BEING READ BY OTHERS. HOW WAS THIS ISSUE ADDRESSED AND RECTIFIED?

35. WHY WAS ADMINISTRATIVE CONTROLS SET TO FULL ACCESS BY CERTAIN EMPLOYEES SUCH AS BOOK KEEPERS AND MONEY HANDLERS? (THEY HAD ACCESS TO EVERYONE'S EMAILS)

36. WHY WAS THE ADMINISTRATOR'S EMAIL ACCOUNT PRE-POPULATED WITH THE MAYORS, H.R., BOOKKEEPERS, FINANCE AND PURCHASING EMAILS ONLY? (ADMINISTRATOR HAD READ/WRITE CONTROL OVER THOSE INDIVIDUAL'S EMAILS).

I UNDERSTAND THAT ANSWERS TO THESE QUESTIONS MAY OR MAY NOT HAVE A SIMPLE ANSWER, BUT I APPRECIATE FULL DISCLOSURE> AGAIN, THANK YOU FOR YOUR COOPERATION.

MONTH OF NOVEMBER 2017 FRAUD/IDENTITY THEFT REPORTS:
I FOUND FIVE FRAUD REPORTS AND TWO IDENTITY THEFT REPORTS. IN EXAMINING ALL OF THE FRAUD REPORTS I FOUND NONE TO APPEAR TO BE RELATED TO THIS INVESTIGATION. I EXAMINED THE IDENTITY THEFT REPORTS AS WELL. THE IDENTITY THEFT REPORTS INVOLVED A POST OFFICE CHANGE OF ADDRESS AND A FRAUDULENT DISCOVER CARD PURCHASE. NONE OF THE FRAUD OR IDENTITY THEFT REPORTS APPEARED TO BE RELATED TO THIS INVESTIGATION.

RESPONSE FROM CONTRACTED I.T. VENDOR C.E.O.:
I RECEIVED, VIA U.S.P.S. MAIL, A PACKET FROM THE PREVIOUSLY CONTRACTED I.T. VENDOR C.E.O. IN REVIEWING ALL OF THE QUESTIONS THAT WERE ASKED AND ANSWERS THAT WERE PROVIDED, NOTHING OF EVIDENTIARY VALUE WAS OBTAINED FROM THE VENDOR.

MONTH OF DECEMBER 2017 FRAUD/IDENTITY THEFT REPORTS:
I FOUND FIVE FRAUDULENT CREDIT CARD PURCHASES AND ONE IDENTITY THEFT REPORT. THE IDENTITY THEFT INVOLVED A DELINQUENT CREDIT CARD BALANCE WHICH THE VICTIM ADVISED HE DID NOT MAKE. NONE OF THESE INCIDENTS APPEAR TO BE RELATED TO THIS INVESTIGATION.

MONTH OF JANUARY 2018 FRAUD/IDENTITY THEFT REPORTS:
I FOUND TWO REPORTS OF FRAUD AND TWO REPORTS OF IDENTITY THEFT FOR THIS MONTH. THE FIRST REPORT OF FRAUD INVOLVED TELEPHONE SOLICITATION AND THE SECOND FRAUD REPORT INVOLVED A CRAIGSLIST PURCHASE. THE FIRST REPORT OF IDENTITY THEFT INVOLVES FRAUDULENT ONLINE PURCHASES WHEREAS THE VICTIM'S MAIDEN NAME WAS USED. THE SECOND IDENTITY THEFT REPORT INVOLVED OPENING UP A FRAUDULENT DIRECT TV ACCOUNT IN THE VICTIM'S NAME. IT DID NOT APPEAR THAT THESE REPORTS ARE RELATED TO THIS INVESTIGATION

MONTH OF FEBRUARY 2018 FRAUD/IDENTITY THEFT REPORTS:
I FOUND THREE REPORTS OF FRAUD AND ONE REPORT OF IDENTITY THEFT. THE FIRST FRAUD REPORT INVOLVED FRAUDULENT ONLINE BUSINESS PRACTICE. THE SECOND FRAUD REPORT INVOLVED AN UNKNOWN PERSON CLAIMING TO WORK FOR A.T.&T. SOLICITING MONEY. THE THIRD REPORT OF FRAUD INVOLVED ANOTHER FALSE CLAIM OF A.T.&T. POSSIBLY CASING RESIDENCE FOR BURGLARY. THE IDENTITY THEFT REPORT INVOLVES AN UNKNOWN PERSON OBTAINING A LOAN IN THE VICTIM'S NAME. IT IS BELIEVED THAT THE INITIAL INCIDENT OCCURRED 8 MONTHS PRIOR BUT THE VICTIM DID NOT BECOME AWARE UNTIL THIS MONTH. I DID NOT FIND ANYTHING IN THE REPORTS THAT WOULD RELATE THESE INCIDENTS TO THIS INVESTIGATION.

MONTH OF MARCH 2018 FRAUD/IDENTITY THEFT REPORTS:
I FOUND FIVE FRAUD REPORTS AND ONE IDENTITY THEFT REPORT. THE FIRST TWO REPORTS INVOLVE MAIL FRAUD. THE THIRD REPORT INVOLVED A TELEPHONE SOLICITATION THAT THE INTENDED VICTIM WON A NEW CAR AND SEND MONEY. THE FOURTH AND FIFTH REPORTS INVOLVED A TELEPHONE "PUBLISHER'S CLEARING HOUSE" SOLICITATION FOR MONEY. THE IDENTITY THEFT REPORT INVOLVED MULTIPLE CREDIT ACCOUNTS OPENED IN THE VICTIM'S NAME. THE ACCOUNTS WERE DISPUTED AND REMOVED FROM VICTIM'S CREDIT REPORT. THIS REPORT DID NOT APPEAR TO BE RELATED TO THIS INVESTIGATION.

04/11/2018:
MONTHLY CONSULT WITH BRIAN YOUNG:
ETHERNET SWITCH DEVICE (ITEM #30) DISCOVERED:
I WAS ADVISED BY BRIAN YOUNG THAT HE WAS INFORMED BY "ADAM" WITH "BCTI" (PHONE VENDOR), THAT "ADAM" HAD DISCOVERED THAT THE MAIN INTERNET FEEDER LINE, RUNNING FROM ROOM #124 TO THE MAIN ANDERSON COUNTY GOVERNMENT SERVER WAS CUT AND SPLICED WHEREAS IT HAD BEEN SET UP WITH FEEDER LINES THAT WERE PLUGGED INTO AN ETHERNET SWITCH. YOUNG STATED THAT IT IS UNKNOWN HOW LONG AGO THE ETHERNET SWITCH WAS INSTALLED, BUT ADDED THAT IT SHOULD NOT BE IN THE MAIN LINE OF THE INTERNET. HE ADDED THAT HE THOUGHT THE MAIN LINE GOING UP TO THE SERVER SHOULD NOT HAVE BEEN CUT AND SPLICED WITH THE ETHERNET SWITCH CONNECTING THE TWO CUT ENDS. BRIAN DESCRIBED THE SPLICING AS FOLLOWS: THE MAIN INTERNET LINE WAS COMPLETELY CUT, THEN A FEMALE ETHERNET PLUG WAS INSTALLED ON BOTH CUT ENDS. TWO SHORT ETHERNET CABLES WERE PLUGGED INTO EACH FEMALE PLUG, THEN BOTH SHORT CABLES WERE PLUGGED INTO THE ETHERNET SWITCH, THUS COMPLETING THE SIGNAL, WITH THE SWITCH SPLICED IN BETWEEN. BRIAN ADVISED THAT NOW THERE WERE THREE OPEN PORTS THAT WOULD ALLOW ANYONE WITH ACCESS TO THE ROOM, TO PLUG A COMPUTER DIRECTLY INTO THE MAIN LINE AND ACCESS THE INTERNET AND/OR ANDERSON COUNTY GOVERNMENT SERVER. IN EXAMINING THE ACTUAL ETHERNET SWITCH I OBSERVED A STICKER AFFIXED TO THE TOP OF THE DEVICE. THE STICKER CONTAINED WHAT APPEARED TO BE A SERIAL NUMBER AND AN ITEM NUMBER.

AFTER MAKING PHONE CALLS TO VENDORS, MYSELF AND BRIAN YOUNG MADE CONTACT WITH STONEY M. HALE II, CONSULTANT FOR BUSINESS INFORMATION SYSTEMS (BIS), (423)773-2566. I QUESTIONED MR. HALE ABOUT THE FOUND ETHERNET DEVICE AND THE SERIAL NUMBER STICKER THAT WAS FOUND ON THE SWITCH. MR. HALE ADVISED THAT THE ITEM NUMBER SOUNDED FAMILIAR AND ADDED THAT HE WOULD HAVE TO CHECK WITH HIS BUSINESS RECORDS AND RETURN MY CALL AFTER CHECKING.

SHORTLY AFTER SPEAKING WITH MR. HALE, HE RETURNED MY CALL AND STATED THAT HE DID, IN FACT LOCATE THAT LISTED ITEM NUMBER IN THEIR RECORDS. MR. HALE STATED THAT IN CHECKING HIS RECORD, HE FOUND THAT BIS HAD SOLD THAT SWITCH TO ANDERSON COUNTY GOVERNMENT AND INSTALLED IT SOMETIME IN 2015. HE STATED THAT HE WOULD HAVE TO HAVE THE SECRETARY PULL THE FILE AND SEE WHO THE TECHNICIAN WAS THAT ACTUALLY DID THE

WORK. I REQUESTED THE BILL OF SALE FOR THE SWITCH, THE WORK ORDER FOR INSTALLING THE SWITCH AND THE REASON WHY IT WAS INSTALLED IN THE MAIN LINE OF THE SERVER. HE ADVISED THAT HE WOULD GET THAT INFORMATION FOR ME AS SOON AS HE COULD.

04/17/2018:

EMAIL FROM BUSINESS INFORMATION SYSTEMS, STONEY M. HALE:

I RECEIVED THE FOLLOWING EMAIL FROM STONEY HALE FROM BIS. THE EMAIL EXPLAINS THAT THE ETHERNET SWITCH WAS LEGITIMATELY INSTALLED. DURING A FOLLOW UP CONVERSATION WITH MR. HALE, I WAS TOLD THAT IT WAS INSTALLED TO ADD THE ADDITION OF A PRINTER FOR THE ANDERSON COUNTY CLERK'S OFFICE.

"GOOD MORNING,

ATTACHED ARE THE SERVICE ORDERS WHERE WE REPLACED THE 5 PORT SWITCH SN 74751 WITH AN 8 PORT SWITCH 79344. THE SWITCH REPLACED IS SN 74751 AND IS ANDERSON COUNTY PROPERTY SINCE WE SOLD IT TO THEM AND DIDN'T HAVE A MAINTENANCE CONTRACT COVERING THIS ITEM. SO WE DIDN'T TAKE THE SWITCH WITH US. THE 8 PORT SWITCH SHOULD BE LOCATED WHERE DECAL18 PRINT ON DEMAND PRINTER IS. UNLESS BRIAN HAS REPLACED THE 8 PORT SWITCH SN79344 WITH A DIRECT CABLE RUN OR SOMETHING ELSE, IT SHOULD STILL BE WITH DECAL18
IF YOU LOOK AT POSTED SERVICE INVOICE.PDF IS WHAT WE SHOW IN OUR SYSTEM AND LETS US KNOW THE ITEM WE ARE GOING TO REPLACE IS THE SN 74751 WITH THE 8 PORT SWITCH 79344.
SAO34383 REVISED.PDF - IS THE 8 PORT SWITCH THAT WAS ADDED TO THE SALES ORDER FOR HOOKING UP NEW DECAL PRINTER
SAO34383-PT.PDF - IS THE ACTUAL PICK TICKET OF DAN INSTALLING THE WORK AND THE 8 PORT SWITCH. AS WELL AS THE ANDERSON COUNTY EMPLOYEE SIGNING OFF ON IT.
SO023379.PDF - IS THE SERVICE ITEM WORKSHEET THAT WE HAVE CUSTOMER SIGN OFF WHEN WE ARE DONE WITH A JOB AND IS WORKING.
I HAVE WHERE WE PURCHASED THE 5 PORT SWITCH SN74751 ON 8/9/2013. THIS WAS ON OUR OLD SYSTEM AND I DON'T HAVE WHERE WE SOLD THIS TO ANDERSON COUNTY THOUGH. I'VE HAD MY GUYS TRY TO FIND IT ON OUR OLD SYSTEM BY THAT SERIAL NUMBER AND MANUFACTURE NUMBER WITH NO LUCK. ONE REASON WE SWITCHED SYSTEMS. I JUST HAVE WHERE WE REPLACED IT IN APRIL OF 2015, AND THIS WAS A PRODUCT WE SOLD ANDERSON COUNTY CLERK. A MAINTENANCE CONTRACT WAS NOT PICKED UP FOR THIS ITEM. SO WHEN IT NEEDED TO BE REPLACED WITH THE 8 PORT SWITCH IT WAS BILLABLE. THE OLD SWITCH IS ANDERSON COUNTY PROPERTY AND OUR GUYS ARE INSTRUCTED NOT TO TAKE EQUIPMENT UNLESS A MAINTENANCE EQUIPMENT AND WE ARE REPLACING UNDER THE MAINTENANCE CONTRACT. ALSO, SOMETIMES CUSTOMERS REQUEST US TO TAKE PCS TO DESTROY HARD DRIVES. NORMALLY WE LEAVE ALL OLD EQUIPMENT FOR COUNTIES TO DISPOSE OF OR TURN OVER TO COUNTY SURPLUS.
IF YOU NEED ANYTHING FURTHER, PLEASE LET ME KNOW! I'M AT A CONFERENCE IN DENVER, CO SO WILL BE LIMITED AVAILABILITY THIS WEEK, BUT SEND ME AN EMAIL AND I'LL RESPOND AS SOON AS POSSIBLE.

HAVE A GREAT DAY,

STONEY M. HALE II
BUSINESS INFORMATION SYSTEMS
SOLUTIONS CONSULTANT"

04/25/2018:

FOLLOW-UP DISCUSSION WITH COUNTY CLERK, JEFF COLE:

AT APPROXIMATELY 0942 HRS. JEFF COLE CONTACTED ME VIA PHONE. I EXPLAINED TO MR. COLE WHY I CONTACTED HIS OFFICE (REQUESTING EXPLANATION ABOUT APRIL 2015 WORK ORDER). I ASKED MR. COLE IF HE KNEW ANYTHING ABOUT THE SPECIFIC WORK ORDER. HE ADVISED THAT IN LATE 2014 HIS OFFICE WAS INSTALLING NEW DECAL PRINTERS TO BETTER SERVE THE COUNTY. HE ALSO STATED THAT THERE WAS WORK BEING PERFORMED AT ALL OF HIS COUNTY OFFICES THAT REQUIRED THE ADDITION OF PRINTERS AS WELL AS OTHER OFFICE EQUIPMENT. I ADVISED MR. COLE THAT THE WORK CONSISTED OF SPLICING AN ETHERNET SWITCH DIRECTLY INTO THE MAIN INTERNET FEED LINE OF THE

SERVER. MR. COLE ASKED IF THE SWITCH WAS IN THE ANDERSON COUNTY SERVER OR THE ANDERSON COUNTY CLERK SERVER. HE WENT ON TO SAY THAT HIS OFFICE, PER STATE REQUIREMENTS, MAINTAINS A COMPLETELY SEPARATE SERVER FROM THE ANDERSON COUNTY GOVERNMENT SERVER AND THAT THERE IS NO COMMUNICATION BETWEEN THE SERVERS. I ADVISED MR. COLE THAT, ACCORDING TO BRIAN YOUNG, THE MAIN SERVER LINE WAS CUT. I ASKED MR. COLE WHO IS MARGARITA BLANTON?. MR. COLE ADVISED THAT SHE WAS THE OFFICE MANAGER FOR THE OAK RIDGE OFFICE. MR. COLE EXPLAINED THAT HIS REASON FOR HER NAME APPEARING ON THE WORK ORDER WAS PROBABLY DUE TO BIS WAS CONDUCTING WORK AT VARIOUS LOCATIONS AND MOST LIKELY FINISHED WORK AT THE OAK RIDGE OFFICE, THE TECHNICIAN WOULD NEED A SIGNATURE AND OBTAINED HER SIGNATURE INSTEAD OF TRAVELING AROUND THE COUNTY FOR VARIOUS SIGNATURES FOR WORK IN THE SAME DEPARTMENT. MR. COLE ADVISED THAT MS. BLANTON NO LONGER WORKS FOR HIS DEPARTMENT.

FOLLOW-UP WITH BRIAN YOUNG:
I HAD A MEETING WITH BRIAN YOUNG ABOUT THE DISCUSSION WITH JEFF COLE. I ASKED BRIAN YOUNG IF HE COULD CONFIRM WHICH ETHERNET LINE WAS ACTUALLY CUT AND SPLICED. HE ADVISED THAT HE MAPPED THE LINE, THEN TESTED THE LINE AFTER WORK HOURS. HE EXPLAINED THAT HE DISCONNECTED THE SPLICED LINE WHICH CUT THE FEED TO ANDERSON COUNTY GOVERNMENT SERVER. I ASKED BRIAN YOUNG WHAT HIS PLAN WAS TO FIX THE CUT LINE. HE STATED THAT AS OF RIGHT NOW, HE INSTALLED A CLOSED PORT SECURE ETHERNET SWITCH WHICH CANNOT BE ACCESSED AS THE PORTS WERE DISCONNECTED. HE STATED THAT HE WILL BE RUNNING A NEW LINE AND WILL BE REMOVING THE SWITCH ALTOGETHER. I THEN INSTRUCTED BRIAN YOUNG TO CONDUCT A SEARCH FOR THE EQUIPMENT LISTED IN THE BIS WORK ORDER. HE ADVISED THAT HE WOULD START WITH THE CLERK'S OFFICE IN OAK RIDGE THEN PROCEED FROM THERE.

AT APPROXIMATELY 1346 HRS. BRIAN YOUNG CONTACTED ME VIA PHONE AND ADVISED THAT HE LOCATED BOTH THE ETHERNET SWITCH THAT WAS INSTALLED TO REPLACE THE 5 PORT SWITCH(EVIDENCE ITEM #30) AS WELL AS THE DECAL PRINTER THAT WAS ALSO INSTALLED AS PER THE WORK ORDER FROM BIS. FINDING THESE ITEMS COOBERATED THE EXPLANATION PROVIDED BY STONEY HALE AND CONFIRMED THAT THERE WAS A LEGITAMATE REASON FOR THE EHTERNET SWITCH TO BE IN ANDERSON COUNTY POSSESSION. IT DOES NOT, HOWEVER, EXPLAIN WHY THE 5 PORT SWITCH WAS FOUND TO BE SPLICED INTO THE MAIN SERVER LINE FOR ANDERSON COUNTY GOVERNMENT. I WILL BE CONDUCTING AN INTERVIEW WITH THE BIS TECHNICIAN THAT PERFORMED THE WORK IN APRIL OF 2015, FOR AN EXPLANATION, BUT AS FAR AS RELEVANCE TO THIS REPORTED INCIDENT, I DO NOT SEE ANY EVIDENCE THAT THE ETHERNET SWITCH WAS INSTALLED FOR ANY OTHER REASON BUT FOR LEGITAMATE PURPOSES.

04/26/2018
FOLLOW-UP PHONE CONFERENCE WITH BIS:
BIS CONFIRMED TO ME THAT THEIR COMPANY HAD SWITCHED OUT THE ETHERNET SWITCH WITH AN UPGRADED ONE. I SPOKE WITH DANIEL SHERMAN, THE ACTUAL SERVICE TECHNICIAN THAT PERFORMED THE WORK. HE ADVISED THAT HE SWITCHED OUT THE 5-PORT ETHERNET SWITCH WITH AN 8-PORT ETHERNET SWITCH. HE THEN ADVISED THAT THE OLD SWITCH WAS LEFT WITH ANDERSON COUNTY CLERK'S OFFICE.

THIS SWITCH WAS SUBSEQUENTLY USED BY BOTH JEFF COLE'S OFFICE AND TIM SHELTON'S OFFICE FOR THE PURPOSE OF PROVIDING BOTH OFFICES WITH AN INTERNET CONNECTION. IN SPEAKING WITH DANIEL SHERMAN AND MICHAEL WILLIAMS, BOTH SERVICE TECHNICIANS FOR BIS, BOTH HAD STATED THAT BIS DID NOT INSTALL THE SWITCH. IT IS UNKNOWN WHO HAD INSTALLED THE SWITCH INTO THE MAIN SERVER LINE.

I ASKED BRIAN YOUNG IF HE HAD RECEIVED ANY REPORTS OF ISSUES REGARDING FRAUD OR IDENTITY THEFT. HE ADVISED THAT HE HAD NOT.

FINAL MONTHLY CHECK FOR FRAUD/IDENTITY THEFT REPORTS:
I FOUND ONE FRAUD REPORT FOR THIS MONTH. THE REPORT CONSISTED OF A FEMALE VICTIM'S DEBIT CARD BEING USED AT SEVERAL LOCATIONS AROUND THE COUNTRY AS WELL AS CANADA. THIS REPORT DID NOT APPEAR TO BE CONNECTED WITH THIS REPORTED INCIDENT. I FOUND ONE IDENTITY THEFT REPORT. THE IDENTITY THEFT REPORT CONSISTED OF THE VICTIM RECEIVING A DEBIT CARD IN THE MAIL FOR A BANK ACCOUNT WHICH HE DID NOT OPEN. NO FINANCIAL LOSS REPORTED IN THIS INCIDENT. THE IDENTITY THEFT REPORT DID NOT APPEAR TO BE RELATED TO THIS CASE.

FINAL CONCLUSIONS AND CASE STATUS (AS OF 04/25/2018):

DURING THE LENGTHY COURSE OF THIS INVESTIGATION, I WAS TASKED WITH DETERMINING IF ANYONE HAD MADE UNAUTHORIZED ACCESS TO ANDERSON COUNTY GOVERNMENT'S SERVER AND ACERTAIN IF ANY DATA OR EMPLOYEE IDENTITY HAD BEEN COMPROMISED. THE INITIAL PHASE OF THIS INVESTIGATION WAS COMPLETED BY THE EARLY PART OF 2017. THE PRIMARY PROBLEM IN DETERMINING IF PERSONNEL HAD THEIR IDENTITY STOLEN IS TIME. I KNEW, FROM PAST EXPERIENCE THAT IT COULD TAKE MONTHS FOR A PERSON TO REALIZE THAT THEIR IDENTITY HAD BEEN TAKEN AND USED CRIMINALLY. I DECIDED EARLY IN THE INVESTIGATION THAT I WOULD HAVE TO CONDUCT MONTHLY CHECKS OF REPORTS AND CONDUCT FOLLOW-UP INVESTIGATIONS INTO ALLEGATIONS OF FRAUD AND IDENTITY THEFT IF IT WAS DETERMINED THAT THE ALLEGATIONS BORE RELEVANCE IN THIS INVESTIGATION. UPON LOCATING A REPORT OF IDENTITY THEFT FROM A COUNTY COMMISSIONER, I FELT IT NECESSARY TO KEEP MY INVESTIGATION OPEN AND EXTEND THE MONTHLY REPORT CHECKS AS WELL AS MEET WITH BRIAN YOUNG ON A MONTHLY BASIS TO ENSURE THAT NO ISSUES HAD ARISEN FROM THE INITIAL COMPLAINT.

DURING MY INVESTIGATION, I LEARNED THAT THE CONDITION OF THE NETWORK FOR ANDERSON COUNTY WAS IN SUCH A POOR STATE, I COULD COMMENT THAT AS A LAYPERSON, I WOULD CONSIDER IT TO BE NEGLIGENT. BELOW IS A REVIEW OF MY FINDINGS:

1. COMMON USERNAMES AND PASSWORDS FOR EMPLOYEE ACCOUNTS AND EMAIL ACCOUNTS.

IT IS WELL KNOWN THAT COMMON USERNAMES AND PASSWORDS FOR ACCOUNTS IS A CONSIDERABLE SECURITY RISK. I WAS ADVISED THAT EMPLOYEE USERNAMES WERE COMMONLY KNOWN BY ALL EMPLOYEES AS WELL AS PASSWORDS, WHICH WERE SIMPLISTIC IN NATURE AND WERE NOT ALLOWED, BY SYSTEM ADMINISTRATOR, TO BE CHANGED. ALTHOUGH NO REPORTS OF EMPLOYEE MISCONDUCT WERE RECEIVED, IT WAS POSSIBLE TO GAIN ENTRY TO OTHER EMPLOYEE ACCOUNTS.

2. THE BARACUDA FIREWALL FOR ANDERSON COUNTY NETWORK WAS SET AND KEPT IN DEFAULT STATUS.

I CONTACTED I.T. COMPANIES AS WELL AS HAD SEVERAL MEETINGS WITH BRIAN YOUNG AND SPOKE TO F.B.I. CYBER CRIMES DIVISION ABOUT THIS ISSUE. IT WAS LEARNED THAT THE BARACUDA FIREWALL IS LESS THAN IDEAL CHOICE OF FOR A COUNTY GOVERNMENT OPERATION, IN AND OF ITSELF, BUT TO ALSO SET UP THE FIREWALL AND LEAVE THE SETTINGS IN A BASIC FUNCTION STATE, WHEREAS I.P. TRAFFIC WITH THE SERVER WAS BEING OVERWRITTEN EVERY 24 HOURS OR LESS, COULD BE CONSIDERED NEGLIGENT. DUE TO THE FACT THAT THE DATA WAS OVERWRITTEN SO QUICKLY, I WAS UNABLE TO OBTAIN AN I.P. LISTING FROM THE REPORTED SUSPICIOUS EVENT TIMEFRAMES.

3. WINDSTREAM INTERNET SERVICE PROVIDER FOR ANDERSON COUNTY DOES NOT MAINTAIN RECORDS.

IN CONTACTING WINDSTREAM COMMUNICATIONS, FOR DATA PRESERVATION AND I.P. ADDRESS TRAFFIC, I LEARNED THAT THOSE PARTICULAR PIECES OF DATA THAT WOULD BE CRUCIAL IN DETERMINING WHEN A COMPUTER ACCESSED OR COMMUNICATED WITH ANDERSON COUNTY NETWORK, WERE NOT KEPT IN ANY DATABASE. I WAS REFERRED TO THE FIREWALL FOR THAT DATA.

4. FEDERAL MS-ISAC REPORT INDICATED NO EVIDENCE OF UNAUTHORIZED ACCESS OR TAMPERING WITH ANDERSON COUNTY GOVERNMENT SERVERS.

UPON RECEIVING ALL THREE REPORTS FROM MS-ISAC, AND COMPARING THE DATA FROM THE REPORTS TO THE INITIAL COMPLAINT FROM HUMAN RESCOURCES DIRECTOR, RUSSELL BEARDEN, I COULD NOT MAKE A DETERMINATION AS TO IF THERE HAD BEEN ANY INTRUSION TO THE COUNTY NETWORK. THE MAJOR EXPLANATION FOR THE SUSPICIOUS ACTIVITY, ACCORDING TO THE DATA IN THE REPORTS, IS NORMAL SYSTEM UPDATING AND NORMAL FUNCTIONS PERFORMED WITHIN THE OPERATING SYSTEM ITSELF. IT SHOULD BE NOTED THAT BRIAN YOUNG, RUSSELL BEARDEN AND GALLAHER & ASSOCIATES DID NOT HAVE ACCESS TO THE INTERNAL SYSTEM ITSELF, AND COULD ONLY OFFER THEORIES WITH THE INFORMATION THAT WAS AVAILABLE IN THE NTFS LOGGING DATA. MS-ISAC WAS ABLE TO

CONDUCT AN IN-DEPTH FORENSIC ANALYSIS OF ALL OF THE HARD DRIVES AND SYSTEMS BEING USED BY ANDERSON COUNTY GOVERNMENT AND COULD EXTRAPULATE AND INTEPRET THE DATA FROM A BASIC LEVEL.

5. BASIC USERNAME AND PASSWORD FOR "LOGMEIN" KNOWN BY SOME COUNTY EMPLOYEES.

I LEARNED DURING MY INVESTIGATION THAT THE REMOTE ACCESS PROGRAM "LOGMEIN" HAD A VERY SIMPLISTIC USERNAME AS WELL AS A PASSWORD THAT WAS SET BY THE SYSTEM ADMINISTRAOR. BOTH USERNAME AND PASSWORD WERE KNOWN TO SOME EMPLOYEES AND COULD ALLOW ACCESS TO THE BADGE SERVER IN ANDERSON COUNTY. IT ALSO WOULD ALLOW SOMEONE ACCESS TO THE MAIN SERVER VIA THE BADGE SERVER. THE USERNAME AND PASSWORD WERE NOT ALLOWED TO BE CHANGED AS WELL, SINCE CHANGING THE PASSWORD WOULD DISRUPT I.T. UPKEEP AND SERVICE, BUT TO WHAT COST IS UNKNOWN.

6. USERNAME AND PASSWORD FOR MAIN SERVER WAS EXTREMELY SIMPLISTIC.

I LEARNED FROM BRIAN YOUNG THAT THE USERNAME AND PASSWORD THAT WAS SET BY THE SYSTEM ADMINISTRATOR, WAS VERY SIMPLISTIC. IF ANYONE HAD THE USERNAME AND PASSWORD, COMPLETE ACCESS WOULD HAVE BEEN GRANTED TO THE NETWORK. THIS ACCESS INCLUDES COUNTY FINANCES, AND ALL EMPLOYEE DATA. TO DATE, I HAVE NO EVIDENCE TO INDICATE THAT DATA HAS BEEN ACCESSED BY UNAUTHORIZED INDIVIDUALS.

7. TERMED EMPLOYEES NOT REMOVED FROM EMAILING AND NETWORK ACCOUNTS.

I RECEIVED INFORMATION FROM BRIAN YOUNG THAT THERE WERE SOME EMPLOYEES THAT WERE NOT EXPELLED FROM THE ANDERSON COUNTY EMAIL SERVER OR THE NETWORK ITSELF. THOSE EMPLOYEES ALSO MAY HAVE KNOWN THE USERNAMES AND PASSWORDS OF AFOREMENTIONED ITEMS, AND COULD HAVE GAINED ENTRY, HOWEVER, THERE ARE NO REPORTS TO INDICATE THAT HAD HAPPENED. SIMPLY ALLOWING PASSWORDS TO BE CHANGED, OR REMOVING ONES ACCOUNT WOULD NOT MAKE THIS AN IMPORTANT ISSUE, BUT THIS TASK WAS REPORTED TO BE NEGLECTED.

8. SPLITTER TYPE DEVICE FOUND PLUGGED INTO PORT #46 OF MAIN SERVER.

THIS PIECE OF EQUIPMENT HAS BEEN A DEBATED SUBJECT BY PERSONS OUTSIDE OF THIS INVESTIGATION. AN EXPLANATION AS TO WHY THE DEVICE WAS BEING USED WILL NEVER BE KNOWN SINCE IT IS UNKNOWN WHO INSTALLED IT. THIS SPLITTER TYPE DEVICE WOULD BE USED TO INCREASE TERMINAL USERS ON THE SAME ASSIGNED PORT AND IF SERVER PORT SPACE IS LIMITED, THEN IT'S USAGE WOULD BE EASILY EXPLANED. THAT BEING SAID, THERE DID APPEAR TO BE PORT SPACE AVAILABLE, SO THE DEVICE FALLS UNDER SCRUTINY. I AM UNABLE TO OBTAIN AN EXPLANATION AS TO WHO INSTALLED THE DEVICE OR WHY.

9. SUSPICIOUS EMAIL DROPDOWN FOLDER MAINTAINED ON ADMINISTRATOR ACCOUNT.

I FOUND THIS PIECE OF INFORMATION VERY TROUBLING. I HAVE NOT BEEN ABLE TO GET ANSWERS FROM THE EMAIL SYSTEM ADMINISTRATOR AS TO WHY THE ADMINISTRATOR HAD THIS TYPE OF ACCESS TO SOME OF THE EMPLOYEE EMAILS. ALTHOUGH THIS ITEM OF INTEREST BEARS NO RELEVANCE TO THE REPORT OF AN UNAUTHORIZED INTRUSION INTO THE ANDERSON COUNTY SERVER, IT WAS FOUND DURING THE COURSE OF MY INVESTIGATION, AND IT'S COMPLETE SIGNIFICANCE WILL NEVER BE KNOWN.

10. ETHERNET SWITCH FOUND IN ROOM #124 OF COURTHOUSE.

THIS IS ANOTHER EXAMPLE OF EQUIPMENT BEING INSTALLED IN THE COURTHOUSE WITHOUT A KNOWLEDGABLE POINT OF CONTACT FROM ANDERSON COUNTY. IN FOLLOWING UP ON THE ORIGIN OF THE SWITCH, I LEARNED THAT BIS HAD ORIGINALLY DESIGANTED THE PIECE OF EQUIPMENT FOR ANDERSON COUNTY CLERK. AT SOME POINT IN THE FUTURE, THE EQUIPMENT NEEDED TO BE UPGRADED. THE PROBLEM IN THIS ISSUE IS THAT ALTHOUGH THE DEVICE WAS USED FOR LEGITIMATE REASONS, HOW IT ENDED UP SPLICED INTO THE MAIN LINE OF THE ANDERSON COUNTY SERVER, IS UNKNOWN.

DURING MY INVESTIGATION, I RECEIVED NUMEROUS REPORTS FROM EMPLOYEES CONCERNING SUSPICIOUS OCCURRENCES AROUND THE WORKPLACE. THESE OCCURRENCES INCLUDED, EMPLOYEES COMPUTERS BEING MOVED BY UNKNOWN PERSONS, EMPLOYEES RETURNING TO THEIR COMPUTER TO FIND THEIR MONITORS ON, WHEN THEY LOCKED THEM PRIOR TO LEAVING, SUSPICIONS OF EMAILS READ WITHOUT THEIR KNOWLEDGE AND NUMEROUS OTHER ISSUES. I HAD TO PRIORITIZE THESE COMPLAINTS AND ADDREES THEM WITH BRIAN YOUNG BEFORE DETERMINING THE VALIDITY OF THE ISSUES AS TO HOW THEY RELATE TO AN UNAUTHORIZED ACCESS TO THE SERVER.

IN CONCLUSION, BY EXAMINING AND INTERPRETING ALL OF THE DATA RECEIVED AS WELL AS BEING MADE AWARE OF THE DEBAUCHED STATE OF THE SERVER AND IT'S SECURITY AT THE TIME OF THE ORIGINAL COMPLAINT, I CAN FIND NO EVIDENCE TO SUPPORT THAT ANDERSON COUNTY GOVERNMENT FELL VICTIM TO AN UNAUTHORIZED INTRUSION INTO ANY OF THE SERVERS. I WAS UNABLE TO FIND ANY EVIDENCE TO SUPPORT THAT ANY COUNTY RESIDENT OR EMPLOYEE HAD THEIR PERSONAL DATA COMPROMISED FROM ANDERSON COUNTY GOVERNMENT. I AM UNABLE TO FIND ANY EVIDENCE TO INDICATE ANY CRIMINAL ACTIVITIES SURROUNDING EX-FILTRATION OF DATA FROM ANDERSON COUNTY SERVERS.

STATUS: CLOSED

INVESTIGATOR DON SCUGLIA