GRANITE NETWORK SECURITY PRESENTATION

BOARD OF EDUCATION MEETING

AUGUST 1, 2017

NETWORK SECURITY CONCERNS

- GRANITE TECHNOLOGY INVESTMENT
- RISKS
- INITIATIVES
- BUDGET IMPLICATIONS

GRANITE TECHNOLOGY INVESTMENT

- GREATER USE OF TECHNOLOGY IN EDUCATING OUR STUDENTS
- GREATER USE OF TECHNOLOGY IN THE DAY TO DAY 'RUNNING' OF THE DISTRICT
- INCREASED NEED TO PROTECT OUR TECHNOLOGY INVESTMENT

GRANITE TECHNOLOGY INVESTMENT

- GRANITE NETWORK CORE
  - TWO DATA CENTERS
    - GEC & GRANGER HIGH
  - 127 PHYSICAL SERVERS
  - 166 VIRTUAL SERVERS
  - 6 FIREWALLS
  - 75 TB FOR STAFF FILES (1 TB IS 1,500 CD'S, 75 TB = 112,500 CD'S)
    - 5.5 MILLION FILES ON SCHOOL/DEPARTMENT SHARES
    - 7.5 MILLION STAFF INDIVIDUAL FILES
  - 96 TB FOR STUDENT FILES
  - 686 TB OF DATA BACKUP (1,029,00 CD'S)
  - MULTIPLE OTHER DEVICES AND SOFTWARE AT THE CORE
  - MOVED INTO THE GEC WITH 6 PHYSICAL SERVERS

GRANITE TECHNOLOGY INVESTMENT

- 114 REMOTE SITE BUILDINGS CONNECTED
- 40,000 DESKTOP COMPUTERS
- 54,000 CHROMEBOOKS
- 2,500 PRINTERS
- 64,000 NETWORK PORTS TO WHICH DEVICES CONNECT
- 2,611 WIRELESS ACCESS POINTS
- 2,250 SECURITY CAMERAS
- COUNTLESS PERSONAL DEVICES

GRANITE TECHNOLOGY INVESTMENT

- 100,000 DEVICES HAVE CONNECTED TO OUR WIRELESS NETWORK (PERSONAL AND DISTRICT DEVICES)
- OVER 30,000 AUTHENTICATED DEVICES AT ANY ONE TIME
- BUILDING ACCESS CONTROL SYSTEMS
- SECURITY CAMERAS
- TIME FORCE BIOMETRIC COLLECTORS
- 4,000 IP PHONES

GRANITE TECHNOLOGY INVESTMENT

- **IOT** (INTERNET OF THINGS: THE INTERNET OF THINGS (**IOT**) IS THE NETWORK OF PHYSICAL DEVICES, VEHICLES, BUILDINGS AND OTHER ITEMS EMBEDDED WITH ELECTRONICS, SOFTWARE, SENSORS, ACTUATORS, AND NETWORK CONNECTIVITY THAT ENABLE THESE OBJECTS TO COLLECT AND EXCHANGE DATA.
  - HVAC CONTROLS
  - FREEZERS
  - BRIGHTSIGN
  - MARQUEES
  - APPLE TV'S, OTHER TV'S, ROKU
  - SPRINKLER SYSTEMS
  - LIGHTING SYSTEMS
  - WEATHER BUGS
    - SOLAR PANEL INTERFACE

GRANITE TECHNOLOGY INVESTMENT

- OTHER EDUCATIONAL DEVICES
  - ENGRAVING SYSTEMS
  - INTERACTIVE WHITEBOARDS
  - GAMING SYSTEMS (X-BOX)
  - 3-D LARGE PRINTERS
  - LARGE FORMAT PRINTERS
  - PLASMA CUTTERS
  - LATHES
  - PAINT MIXERS

GRANITE TECHNOLOGY INVESTMENT

- OTHER EDUCATIONAL DEVICES
  - SCOPE CAMERAS
  - TIRE BALANCERS
  - ALIGNMENT MACHINES
  - FRAME RACK STRAIGHTENER
  - COMPUTER NUMERIC CONTROL MILLING MACHINE (3D LATHE)
  - CAR SCANNING/DIAGNOSTIC TOOLS

GRANITE TECHNOLOGY INVESTMENT

- 9,813 STAFF ACCOUNTS
- 67,127 STUDENT ACCOUNTS
- 32,964 PARENT ACCOUNTS

GRANITE TECHNOLOGY INVESTMENT

- NETWORK UTILIZATION
  - 588,700 INCOMING EMAILS DAILY (GRANITESCHOOLS.ORG ONLY, GRANITESD.ORG NOT FILTERED BY GRANITE) (GRANITESCHOOLS.ORG NUMBERS ONLY, GRANITESD.ORG IS NOT FILTERED BY GRANITE)
  - 63,200 OF THE DAILY INCOMING DELIVERED (10-11% LEGIT EMAILS)
  - 38 MILLION EMAILS ARCHIVED OVER THE PAST 15 MONTHS
  - OUTGOING DATA OF 8-9 GB AT PEAK TIMES (1 GIG = 20 YARDS OF BOOKS ON A SHELF, 9 GB IS ABOUT THE LENGTH OF 2 FOOTBALL FIELDS OF BOOKS, PER SECOND)
- APPLICATIONS DEFINED IN LANDESK
  - 560 DEFINED SOFTWARE APPLICATIONS
  - 400 WEB APPLICATION LINKS
- GRANITE'S NETWORK ONE OF THE TOP TRAFFIC-GENERATING NETWORKS
  - 1ST – UNIVERSITY OF UTAH
  - 2ND – UTAH STATE UNIVERSITY
  - GSD 3RD OR 4TH
  - LARGEST K12 GENERATING NETWORK

RISKS

- INCREASE IN CYBER CRIMINAL ACTIVITIES
  - HTTP://WWW.EDWEEK.ORG/EW/ARTICLES/2017/01/11/RANSOMWARE-ATTACKS-FORCE-SCHOOL-DISTRICTS-TO.HTML
  - SALT LAKE SD DDOS ATTACK (DENIAL OF SERVICE)
  - GSD SIMILAR ATTACK FIRST DAY OF SCHOOL 2015 (UNPUBLICIZED)
  - GSD HAD CASES OF RANSOMWARE OF USER FILES
    - KITCHEN UNABLE TO PERFORM FINANCIAL TRANSACTIONS FOR 1.5 DAYS
- UETN ASSESSED GSD RISKS AND VULNERABILITIES
  - MAY 2016

MOST RECENT CYBER ATTACKS

- COMPREHENSIVE HIGH SCHOOL HACK
- SIMILAR HACKING AT OTHER SECONDARY SCHOOLS

GENERALIZED CYBER ATTACKS

- **PHISHING** IS THE ATTEMPT TO OBTAIN SENSITIVE INFORMATION SUCH AS USERNAMES, PASSWORDS, AND CREDIT CARD DETAILS, OFTEN FOR MALICIOUS REASONS, BY DISGUISING AS A TRUSTWORTHY ENTITY IN AN ELECTRONIC COMMUNICATION.
- **MALWARE**, SHORT FOR **MALICIOUS SOFTWARE**, IS AN UMBRELLA TERM USED TO REFER TO A VARIETY OF FORMS OF HOSTILE OR INTRUSIVE SOFTWARE INCLUDING COMPUTER VIRUSES, WORMS, TROJANS HORSES, RANSOMWARE, SPYWARE, ADWARE, SCAREWARE, AND OTHER MALICIOUS PROGRAMS. IT CAN TAKE THE FORM OF EXECUTABLE CODE, SCRIPTS, ACTIVE CONTENT, AND OTHER SOFTWARE. MALWARE IS DEFINED BY ITS MALICIOUS INTENT - ACTING AGAINST THE REQUIREMENTS OF THE COMPUTER USER - AND SO DOES NOT INCLUDE SOFTWARE THAT CAUSES UNINTENTIONAL HARM DUE TO SOME DEFICIENCY.

CURRENT SECURITY PROTECTIONS

- SPAM/VIRUS PROTECTION ON GRANITESCHOOLS.ORG ACCOUNTS
- MICROSOFT FOREFRONT SECURITY FOR DEVICE PROTECTION
- FIREWALL INCOMING SCANNING FOR BAD CONTENT
- REDUNDANCY IN WIRELESS NETWORK BETWEEN TWO DATA CENTERS FOR FAIL OVER (80% OF NETWORK TRAFFIC COMES FROM GSD WIRELESS NETWORK)
- UPDATING OF COMPUTER OPERATING SYSTEMS/PATCHES

UETN FINDINGS

- PENETRATION TEST OUTCOMES @ GEC ONLY
  - FOUND DOCUMENTS ON UNSECURED COPIERS/PRINTERS
  - SUCCESSFUL DELIVERY OF 4 SEPARATE PHISHING EMAILS TO USERS
  - SUCCESSFUL CREDENTIAL HARVESTING OF 14 USERS FROM WIRELESS NETWORK
  - SUCCESSFUL CREDENTIAL HARVESTING OF 36 ACCOUNTS FROM ATTACHED NETWORK
- CONCLUSION: HARD OUTER SHELL, SOFT, CUSHY INSIDE

UETN SUGGESTIONS

- FOLLOW AN ESTABLISHED SECURITY FRAMEWORK
  - CENTER FOR INTERNET SECURITY CRITICAL CONTROLS (CIS CONTROLS)
- SEGMENT NETWORK
- IMPLEMENT SECURITY POLICIES AND PROCEDURES

GSD CURRENT FOCUS

- IMPLEMENT BASE CENTER FOR SECURITY CONTROLS CRITICAL CONTROLS 1-5
  - CSC 1 : INVENTORY ALL DEVICES
  - CSC 2 : INVENTORY ALL SOFTWARE
  - CSC 3 : SECURE DEVICE CONFIGURATIONS
  - CSC 4 : PERFORM CONTINUOUS VULNERABILITY ASSESSMENT
  - CSC 5: CONTROL ADMINISTRATIVE PRIVILEGES

COMMITTED RESOURCES

- $245,705.80 CISCO COMPUTER EQUIPMENT (TO PROFILE AND POSTURE 10,000 OF THE ESTIMATED 100,000 DEVICES)
- ORIGINAL QUOTE TO PROFILE AND POSTURE 100,000 DEVICES WAS OVER $800,000
- $196,296 COMPUTER SWITCHES
- NO TOOL TO MEET CSC-4 TO MONITOR AND PERFORM ON GOING RISK ASSESSMENTS
- NO TOOL TO MEET CSC-2 TO INVENTORY SOFTWARE ON DEVICES

UPCOMING IMPLEMENTATIONS

- REMOVE STAFF ADMINISTRATIVE RIGHTS TO COMPUTERS (CSC 5) TO DECREASE LIKELIHOOD OF USERS INSTALLING MALWARE (AUGUST 1ST)
- INVENTORY ALL DEVICES; ALLOW ONLY KNOWN DEVICES TO ATTACH TO NETWORK (CSC 1)
  - EVERY DEVICE WILL HAVE A PROFILE
  - EVERY DEVICE MUST CONFORM TO A POSTURE (DEVICE STANDARD)
    - DEVICES MUST HAVE CURRENT OPERATING SYSTEM AND BE PATCHED
    - DEVICES MUSH HAVE ANTI-VIRUS SOFTWARE
- REFINE WIRELESS NETWORK FOR EDUCATIONAL USAGE
- CHANGE COMPUTER IDLE TIME TO 20 MINUTES

IMPACT OF IMPLEMENTATIONS

- USERS WILL NO LONGER HAVE ABILITY TO INSTALL THEIR OWN SOFTWARE
  - MUST COORDINATE WITH STS/LMETS OR INFO SYSTEMS STAFF FOR INSTALLATION
  - SOFTWARE APPROVAL LIST/PROCESS WILL BE ENFORCED
  - USERS CAN INSTALL ANY APPLICATION CONTAINED IN LANDESK
- CANNOT CONNECT JUST ANY DEVICE TO THE NETWORK; NO PROFILE – DEVICE CANNOT CONNECT
  - LIMITS THE CONNECTION OF PERSONAL DEVICES
  - LIMITS THE PURCHASE THEN CONNECTION OF RANDOM DEVICES TO THE NETWORK
  - ANY DEVICE MUST PASS PROFILE AND POSTURE TESTS TO CONNECT TO NETWORK (WE MUST KNOW WHAT DEVICE IS, AND IT MUST MEET MINIMUM STANDARDS)
- LIMITS PERSONAL DEVICE CONNECTIVITY TO WHAT WE CALL GSDSECURE TODAY
- GSDSECURE PRIORITIZED FOR EDUCATIONALLY PURPOSED DEVICES

WHAT WE CAN'T PROTECT AGAINST

- USER IGNORANCE OR LACK OF PERSONAL SECURITY

QUESTIONS/COMMENTS