EVERY SERVER, EVERY DEVICE, EVERYONE AND MORE….

THE RANSOM OF MERCER COUNTY TECHNICAL SCHOOL

Deborah Donnelly, School Business Administrator and Board Secretary

Frederick J. Hillman, IV, CEFM, Manager: Information Technologies/Facilities and Grounds and School Safety Specialist

*Note: Both panelists hold their respective positions for the Mercer County Technical Schools and the Mercer County Special Services School District.

TRUTH IS STRANGER THAN FICTION MARCH,2020

March 2020 - COVID-19 Planning Consumes Us

Monday the 9th

- Discover that the technical Schools entire information technology structure is being held hostage by a hacker.
- Teacher sent home due to a fever.

Tuesday the 10th

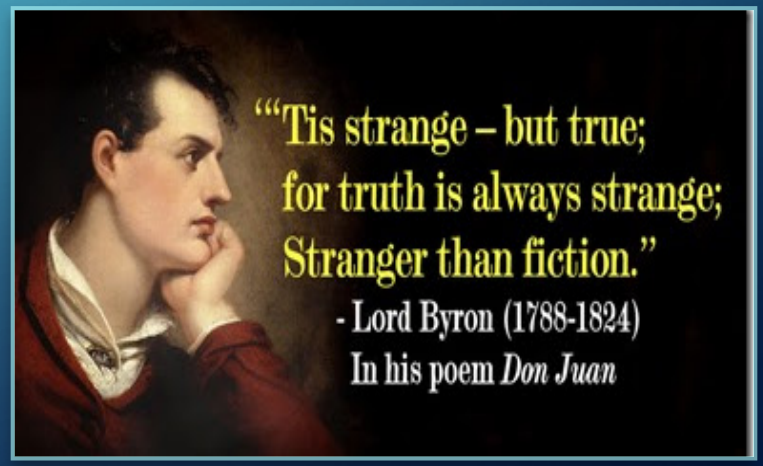
- Hot Water Heater exploded in HS no water plant wide but the fire is out.
- Bus Accident at the Capello School - full bus.

Saturday the14th

- Notified teacher is positive for COVID-19.

Monday the 16th

- Governor Closes Schools as of the 18th



CAUGHT BETWEEN TWO FREIGHT TRAINS

WEEK OF MARCH 9,2020

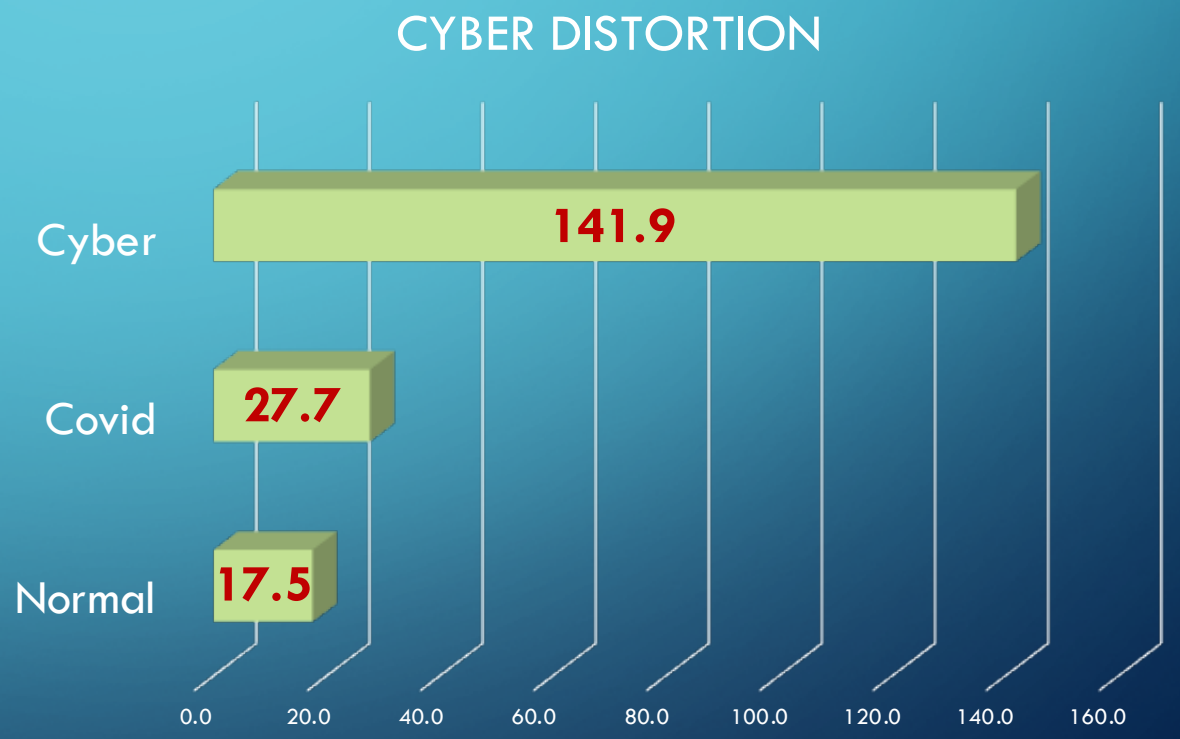
Which will consume us; COVID-19 Rumbler or the CYBER Express?

Time spent first two weeks.

Normal	Covid	Cyber
9%	15%	76%
17.5	27.7	141.9

187.1 Total Hours

4.68 Equivalent Weeks



DISTORTION

Distortion definition is - the act of twisting or altering something out of its true, natural, or original state: the act of distorting.

*https://**www.merriam-webster.com**/dictionary/**distortion***

CYBER CLAIMS DISTORT YOUR WHOLE OPERATION

MONDAY
MARCH 9,2020

CYBER DAY 1 EARLY
5:30 AM TO 7:00 AM

05:30 Arrive for Day
06:17 SMS from Superintendent – can't access MCTS email
06:20 Checked email access to emailserver.mcts.edu – unresponsive
06:20 Verified MCSSSD email was up.
06:30 Able to RDP to MCTS email server, unable to launch management console
06:31 Noticed several files with .ruyk extension.
06:32 Found ryukreadme.html
06:40 Checked other servers in domain and found all were encrypted.
06:57 Notified Superintendent, via SMS it appears district was a victim of a ransomware attack.
07:00 Notified School Business Administrator of attack via phone.

MONDAY
MARCH 9,2020

CYBER DAY 1 CONTINUED
7:01 AM TO 8:49 AM

07:01 Notified Custodial Supervisor/Custodial Staff to stay off Wi-Fi and that services may be down.

07:02 Completed online Cyber Claim Form SPELL JIF.

07:03 Started to go through servers in detail to see what was effected.

08:09 Notified by Custodians that online clocks may be down keep track of time by hand.

08:28 Notified SPELL JIF of apparent Ransomware Attack.

08:31 Phoned Connell Foley Breach Line – followed directions to call Cell Phone

08:32 Phone 862-485-5802 left VM about suspected breach.

08:49 Phone call with KR of Connell Foley reviewed facts, was directed to shut down internet by pulling network cables. Pulled ASP, Directed HP to direct CT to pull HCC and AG to pull SYP.

MONDAY
MARCH 9,2020

CYBER DAY 1 CONTINUED
9:00 AM TO 8:15 PM

09:00	COVID-19 LEADERSHIP MEETING @ 1085
NOTE:	INSTRUCTIONAL STAFF MEMBER SENT HOME DUE TO FEVER.
10:12	CALLED ASP CUSTODIAN TO ADVISE NO CLOCK FOR SEVERAL DAYS LET STAFF KNOW TO KEEP TRACK OF HOURS WORKED.
11:00	COVID-19 PRINCIPAL MEETING @ 1020.
11:30	CALL - CONFERENCE BRIDGE WITH CF, IRG, AND STARR RE: INCIDENT.
13:00	COVID-19 PRINCIPAL MEETING @ 1085.
13:44	EMAILED H1N1 LETTER TO SBA.
15:41	EMAILED COVID-19 CLEANING PROCEDURES TO SBA.
15:58	CALL TO SPELL UPDATE ON PLAN OF ACTION FROM CONFERENCE BRIDGE.
16:15	PHONED ERCO SETUP INSTALL MONDAY OF SPRING BREAK.
17:03	CALL TO SBA UPDATED ON STATUS.
17:17	SUPERINTENDENT PHONED UPDATED ME ON COVID-19 PLAN AND CONFERENCE WITH STAFF MEMBER (MERCER COUNTY), ASKED QUESTIONS ABOUT RANSOMWARE SO SHE COULD UPDATE COUNTY. SHARED INFO FROM CONFERENCE BRIDGE.
17:23	PHONE CALL FROM DL WILL RETURN FROM SICK LEAVE AS OF 3/16/19
17:30	BEGIN DATA COLLECTION FOR IRG
20:15	DEPART

TUESDAY
MARCH 10, 2020

CYBER DAY 2 EARLY
5:30 AM T0 9:00 AM

05:30 Arrive
06:00 Export and update data collection to IRG FTP site (Cyber).
07:00 Check Buildings for COVID19 response re: Extra Cleaning. (COVID).
08:39 Phone call from SH – ASP HWH exploded, fire out, no hot water campus wide. (Property).
08:40 Phoned MTC requested Service Call for HWH at ASP. (Property).
08:45 Arrived at SSSD Tech Office (Daily Routine).
09:00 Report of Bus Accident at JFC (**Bus Accident**).

TUESDAY MARCH 10,2020

CYBER DAY 2 CONTINUED

9:05 AM TO 10:00 AM

09:05 Onsite at Bus Accident, 1 Bus vs. Concrete barrier – Bus Missing Left Front Tire, 5 Students on board, plus driver and bus aide. SSSD staff onsite: JF – Transportation, RH, ML, AK - B&G, BW– MCSO Guard. (**Bus Accident**).

09:20 Phone HTPD 609-581-4000 asked if dispatch on the way. Advised, "in the que." (**Bus Accident**)

09:21 Phoned SBA updated on no injuries, advised children removed. No list of names or seat positions, JF was working on getting both of them. (**Bus Accident**).

09:22 Phoned HTFD Fire Marshal to inquire if Fire in route. (**Bus Accident**).

09:26 Email from RM with updated property claim – HWH ASP. (Property).

09:40 Phone Call from: ePlus re: Configuration of Office 365 (Cyber).

09:40 HTPD onsite – Officer Jeff Galant # 472 Case: 20-09662 (**Bus Accident**).

09:51 Advised SBA that police on site but no emergency staff asked RC to call 911 to send kids to hospital to get checked out. Also advised parents not yet called. Attend to internal difficulty over accident procedures. (**Bus Accident**).

10:00 Phone ML advise that wrecker is in route. (**Bus Accident**).

TUESDAY MARCH 10, 2020

CYBER DAY 2 CONTINUED *10:13 AM T0 NOON*

10:13 On scene at bus accident working out details of medical triage with Nurse, Principal, SBA and Superintendent. (**Bus Accident**).

10:40 Wrecker onsite. (**Bus Accident**).

10:57 Sent excel spreadsheet with names for replacement email addresses to build temp or replacement email server for MCTS. (Cyber).

11:09 Call Supt to advise News helicopters overhead. (**Bus Accident**).

11:13 Emailed GB copy of Dell PO for new servers at MCTS to send to Dell. (Cyber).

11:37 Emailed draft press statement for Bus Accident. (**Bus Accident**).

11:41 Call from Vendor re: Floor Install-ASP (Property).

TUESDAY
MARCH 10, 2020

CYBER DAY 2 CONTINUED
2:30 PM TO 1:48 PM

12:30 Call MES Principal re: COVID Planning - Chromebooks. (COVID).

12:32 Call MHS Supervisor re: COVID Planning - Chromebooks. (COVID).

12:46 Sent GB Dell Customer Number for Dell order. (Cyber).

12:59 Call Cyber Attorney – Status update, phones restoration. (Cyber).

13:08 Call - Update Sypek Principal timeline for phone restoration. (Cyber).

13:11 Call – SBA re: Phone Outage (Cyber).

13:12 Call – HP – Network hard drives down – (Cyber).

13:22 Call Cyber Attorney – Status update – network secured (Cyber).

13:48 Emailed JW at Dell re: Ship to address to MCSSSD. (Cyber).

TUESDAY
MARCH 10, 2020

CYBER DAY 2 CONTINUED
2:00 PM TO 7:15 PM

14:00 Plumber onsite – ASP HWH (Property).

14:03 Call – Update Adjustor on HWH Claim (Property).

14:45 Meet ASP Principal re: HWH- Hand Sanitizer deployed to bathrooms. (COVID).

15:15 Meet with SBA, Conference call with ST @ SPELL (Cyber).

15:30 Meet with SBA, Conference call with KR Cyber Counsel. (Cyber).

15:45 Secure Backup of Budget, Accounting, Payroll and Personnel, verify functionality of VPN system. (Cyber).

18:54 Emailed RM copy of invoice for Insurance Claim for HWH ASP. (Property).

19:15 Depart for Day

WEDNESDAY
MARCH 11, 2020

CYBER DAY 3

ORDINARY BUSINESS MATTERS - Review emails, sign and approve invoices and reports; Out of Range Fridge in Baking @ Sypek; Reed School Coverage; Service Call Placed – Locksmith – Sypek BR Door.

CYBER - SMS Superintendent with Update; 90 minute Conference Bridge with KR, Superintendent, SBA and IRG; Onsite HCC copy artifacts as required by IRG; Onsite MCTS - Continue review of servers and workstations, collect additional artifacts; New Email Server for MCTS up, account information sent to Staff – email services restored; IRT onsite at ASP, met with team reviewed incident and provide backed information; continue gathering documentation for IRT.

COVID-19 - Meet with B&G Leadership Team re: Planned COVID Cleaning and response to pandemic; Staff Meeting brief staff on COVID Plan. ASP Staff Meeting brief staff on COVID Plan.

Property Claim -Meet Adjustor on ASP HWH

20:15 PM Depart

SATURDAY & SUNDAY MARCH 14 & 15, 2020

A DIFFICULT *WEEKEND*

- Advised that an instructional staff member at MCSSSD tested positive for COVID-19.
- The staff member worked in our elementary school and was exposed to a person with COVID-19 on March 1, 2020. Our instructor worked March 2nd through 6th and then March 9th before being sent home with a fever.
- Spent Saturday immersed in discussions internally and externally.
- Worked Sunday managing communications internally and externally, working directly with the Board of Health, the JIF and various contractors to sanitize and prepare the facilities for school on Monday, March 16, 2020.

MONDAY - FRIDAY MARCH 16 & 15, 2020

A DIFFICULT *WEEKEND*

March 16, 2020

07:00 Onsite

07:30-18:15 IRT onsite work with them. (CYBER – 13 Hours)

12:00 Governor Conference Call re: School Closures (COVID)

13:00 District Conference Call re: School Closures (COVID)

18:15 Depart 06:15

March 17, 2020

06:30 Onsite

07:30-21:45IRT onsite work with them. (CYBER – 13 hours)

13:00 District Conference Call re: School Closures (COVID)

21:45 Depart

March 18, 2020

06:15 Onsite

07:00-19:00IRT onsite work with them. (CYBER – 12 hours)

17:00 Depart

MARCH 23, 2020 THROUGH

INCIDENT REPONSE TEAM DONE

- Between 12:30PM on March 11, 2020 and 6:00PM on March 21,2020 Incident Response Team removed, and replaced and reformated @ 500 device drives on all workstations throughout the district, and rebuilt 19 virtual servers running on 6 physical hosts.
- Help is gone, now the real work starts.
- District Closed to Students 3/13/20, no staff onsite except B&G!
- Technicians working remote until 05/18/2020

CURRENT STATUS – STILL NOT DONE

Item	Current Status
Restore Temporary Email Services to Staff (New Domain)	Completed on March 10,2020
Prepare inventory of existing hardware	Completed on March 10, 2020
Order new hard drives for all systems & servers	Completed on March 12, 2020
Restored VOIP Phone Services	Completed on March 16, 2020
Restore AD Structure and Domain Controllers	Completed on March 16, 2020
Deployed Endpoint Detection & Response (Sentinel One)	Completed on March 16, 2020
Migrated Student Devices into Student VLAN	Completed on March 18, 2020
Configured temporary DHCP Servers	Completed on March 19, 2020
Configured and deployed NGFW PA-3220	Completed on March 26, 2020
Restore services to Door Controls & CCTV Systems	Completed on March 31, 2020
Restored Basic Network Services District wide	Completed March 31, 2020
Transferred & Restored Email to Google for original domain	Completed April 1, 2020

CURRENT STATUS – STILL NOT DONE

Item	Current Status
Replaced aging network switch gear , migrate to fiber wide area network.	Completed May 1, 2020
Remove and scrap and dispose of all old servers	Completed May 15, 2020
Reimage and install Software for Administrative Workstations	Completed May 15, 2020
Reimage and Install Software for Staff Workstations	Almost done, should be completed by 8/1/20
Reimage and Install Software for Student Workstations	In Process – Target Completion 8/20/20
Build GPO, and Student AD	In Process – Target Completion 8/20/2020
Rebuild & Configure Helpdesk Server(WHD – Solar Winds)	In Process – Target Completion 8/20/20
Rebuild & Configure Monitoring Server(Intermapper)	In Process – Target Completion 9/15/2020
Deploy Classroom Management Solution(GoGuardian)	Product Selected – Target Date 9/30/2020
Deploy CASB Solution to Manage Cloud Assets(Cloudlock)	Product Selected – Target Live Date 10/15/20
Deploy Backup Solution for Onsite and Cloud Files	Starting Investigation – Target Date 11/15/20
Deploy Security Awareness Training/Phisher(KnowB4)	Product Selected – Target Date 9/30/2020

TAKE AWAYS

1. Whatever you are doing relative to Malware/AntiVirus – Stop and deploy an EDR now!
2. Implement Security Awareness Training and phish your instructional staff and administrative staff.
3. Make sure your backup:
    1. Can actually be restored by testing restoration, often.
    2. Is Air Gapped and not part of your domain.
    3. Train your IT Staff how to handle a suspected malware attack(Remove from Network)