Committee Purpose

James M. Heiser, CPA

Chair, Spell JIF IT/Cyber Committee

Delanco Township School District – Business Administrator/Board Secretary

Moorestown Township School District – Assistant Business Administrator

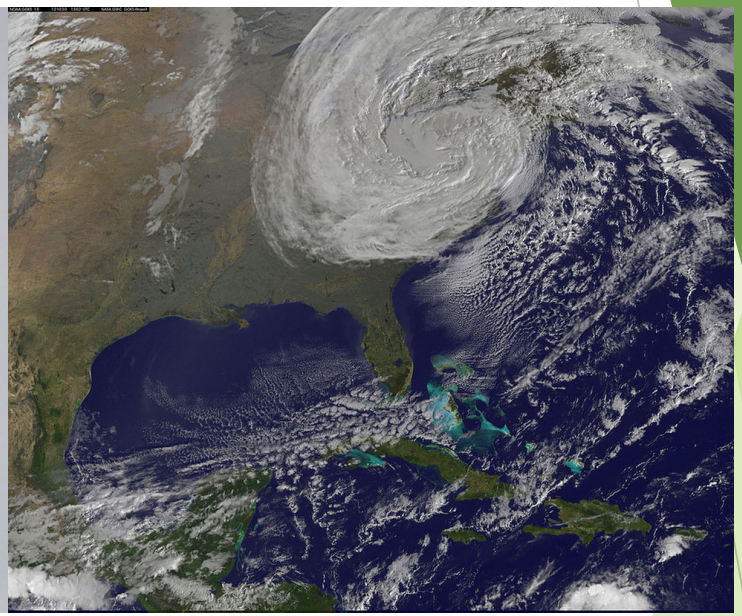
Committee of “How”

- We are a committee of “how” NOT “no”
  - How can we purchase new technology (educational software, facilities controls, servers, etc.) while also understanding the maintenance and risks associated with the purchase?
- Primary purpose and mission is to provide members with information and resources to help reduce the risk of a toxic cyber event while promoting a culture of positive cyber hygiene
- As our technological footprint grows larger and larger at an even faster rate, we must take a collaborative approach to cyber security

Ransomware Attack

- Started new job on Monday, January 9, 2017
- Friday the 13th – New meaning to me
- On Friday, January 13, 2017, arrived at work and was unable to access accounting or personnel systems
- Contacted IT Department and was informed they were working on it
- IT Department contacted me informing me that files were encrypted and they were taking our systems offline to determine how significant the issue was
- Immediately thereafter called insurance company to inform them of the issue and a “triage” call was set up
- Insurance company set up a conference call with an approved attorney that specializes in cyber security events and data privacy
- Local Police Department, State Police Department, and FBI were contacted to inform them of the issue

Storm is Coming



Ransomware Attack (Cont'd)

- Attorney recommended appointing a company that specializes in forensic investigating and cyber defense
- IT Department worked around the clock and on January 17th, our network was brought back online after being down for approximately two and half operating days
- District provided virtual machine disks of breached server with all snapshots, all database logs available, all firewall logs, and all security, system, and remote access logs from our domain controller
- Business Department discovered that 3 months of data was missing and we were only able to back up to October 2018
- Began the process of building the accounting and personnel system back to date (reentering receipts, bill lists, purchase orders, new hires, etc.)
- On February 21, 2019, forensic team determined confidential information COULD have been seen
- Attorney began immediately analyzing the findings and had to determine individual State laws in relation to disclosing the issue

Ransomware Attack (Cont'd)

- Business Office provided numerous server files to determine the individuals and vendors that needed to be provided with notification
- Additional authorities were contacted to inform them of the breach (i.e. additional State Police Departments)
- Attorney drafted letter to notify ALL (past and present) employees and vendors of the breach
- District appointed company to setup a call center, offer credit monitoring services, and coordinate the mailing of all notifications
- On May 26, 2019, letters were mailed out and phones began ringing continuously

Delanco Township School District
Walnut Street Middle School
M. Joan Pearson Elementary School

RE: Notice of Data Security Incident

Dear [Recipient Name]:

I am writing to inform you that the Delanco Township School District ("Delanco") recently discovered an incident that may affect the security of your personal information. We are providing this notice to ensure that you are aware of the incident so that you may take steps to protect your information should you feel it is appropriate to do so.

What Happened? On January 13, 2017, Delanco discovered that a server holding certain employee and vendor data had been affected by a ransomware program that encrypted certain files on the server. Delanco immediately began work to restore the affected files and launched an investigation, with the assistance of a forensic investigation firm, to determine what had happened, what data may have been subject to unauthorized access, and to ensure that our network was secure.

What Information Was Involved? On February 21, 2017, we determined that certain employee and vendor data may have been subject to unauthorized access on January 13, 2017. The information related to you that may have been subject to unauthorized access includes your name, address and Social Security number. Your bank account information may have also been subject to unauthorized access.

What We Are Doing. Immediately after discovering the ransomware incident, we took steps to prevent any potential unauthorized access and launched an investigation into the event. Delanco takes the security of your personal information very seriously. We are offering you complimentary access to 12 months of free credit monitoring and identity restoration services. The enclosed *Steps You Can Take To Protect Against Identity Theft and Fraud* contains instructions on how to enroll and receive these free services, as well as information on what you can do to better protect against identity theft and fraud. We are also notifying certain state regulators of this incident.

Total Cost of Ransomware Attack

- Appointment of Special Counsel that specializes in cyber attacks – $18,850.00
- Appointment of forensic team to determine what data may have been compromised – $13,500.00
- Credit Monitoring Services - $3,500.00
- Phone ringing off the hook for two weeks straight - PRICELESS
- Data Loss Information – Three months of transactions in accounting system had to be reentered and reconciled. Forensic audit determined confidential information COULD have been seen
- Total Business and IT Department Hours Lost – 360 hours spent bringing system back up to date and getting all systems back online
- Impact on Instruction – Internet access taken down for two and a half operating days

Uncomfortable Issues