



Northern Burlington County
Regional School District

Breach Story

Richard Kaz, Business Administrator
Steve Lee, Director of Technology

- 
- Burlington County
 - 7-12 Regional School District
 - Chesterfield, Mansfield, North Hanover, Springfield, and JBMDL
 - 2250 Students
 - 2 Schools
 - Support all four constituent districts
 - Three of the constituent districts rely on NB for internet connection



Day One

June 1, 2021

Tuesday

The Day after Memorial Day Weekend

In Person Instruction

Ransomware

A person wearing a dark hoodie is centered in the frame. Their face is obscured by a bright, glowing green light that forms a rectangular shape, suggesting a screen or a digital interface. The background is a dark teal color filled with a dense pattern of green binary code (0s and 1s) that appears to be falling or scrolling, similar to the 'Matrix' effect. The overall mood is mysterious and technological.

6:30 AM

Report that the transportation routing application is not functioning



6:35 AM

VPN into the application server from
home to investigate

Ransomware



6:35 AM

YOUR FILES ARE ENCRYPTED
Your photos, documents and other important
files have been encrypted with unique key,
generated for this computer.

NEXT



7:00 AM

Notified the business administrator

Ransomware

A person wearing a dark hoodie is centered in the frame. Their face is obscured by a bright, glowing green light that forms the shape of a face. The background is a dark teal color filled with a pattern of binary code (0s and 1s) in a lighter green color. The text "8:00 AM" is overlaid in the center in a large, white, sans-serif font.

8:00 AM

Business administrator notified
insurance company



8:00 AM

Director of technology arrive at the
district

Ransomware

A person wearing a dark hoodie is shown from the chest up. Their face is completely obscured by a glowing blue digital grid pattern. The person's right hand is raised, with fingers spread, as if gesturing or typing. The background is a dark blue gradient filled with a dense, glowing pattern of white and light blue binary code (0s and 1s).

8:00 AM

Technology department continues to
assess the damage

10:00 AM

Changed all domain admin account passwords
Isolated unimpacted servers from the network

Ransomware

A person wearing a dark hoodie is centered in the frame. Their face is obscured by a bright, glowing green light that forms the shape of a face. The background is a dark teal color filled with a pattern of binary code (0s and 1s) in a lighter green color. The overall aesthetic is digital and mysterious.

12:30 PM

District's first meeting with the breach coach and the forensics/remediation firm

DAY ONE

Technology department spent most of the day
and well into the night to deploy
forensics/remediation tools

Ransomware

Impacted Services

A person wearing a dark hoodie is shown from the chest up. Their face is completely covered by a white grid pattern, making them unrecognizable. They are holding up their right hand with fingers spread. The background is a dark blue-grey color with a faint, glowing binary code (0s and 1s) scattered throughout, giving it a digital or cyber-themed appearance.

- Bus Routing Application Server
- One Domain Controller
- One File Server

Forensic and Remediation Processes

- Forensics of all devices
- Monitoring of all devices
- Negotiation with the threat actor
- Monitoring the dark web for exfiltrated data



Forensic Result

Data was exfiltrated

Forensic Result

Personally Identifiable
Information (PII) was included in
the data theft



Restoration Process

Backup

- Local and remote backups were examined and verified to be uncontaminated
- The latest backups were restored
- All impacted servers were back online within a week

Restore



Communications

The background is a teal-colored illustration depicting a networked communication environment. It features silhouettes of several people at the bottom, with white circles on their heads connected by a web of lines to various icons above. These icons include a smartphone, a laptop, a lightbulb, a speech bubble, a globe, a cloud, a play button, a gear, a document, a bar chart, a magnifying glass, a pencil, and an envelope. The overall theme is digital communication and collaboration.

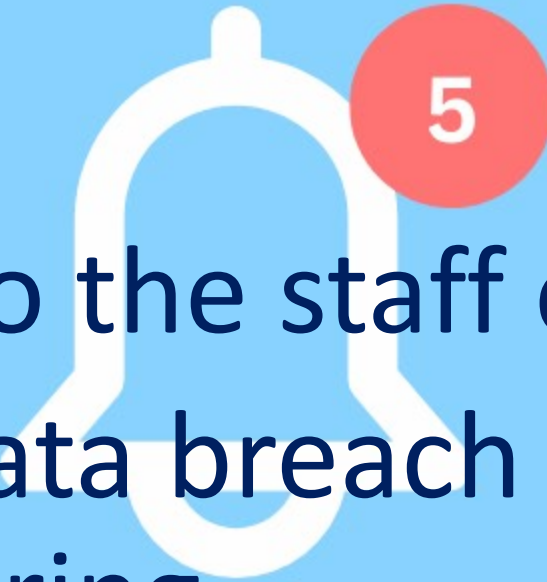
- Breach Coach
- Forensics/Remediation Firm
- Ransom Negotiator
- Insurance Company

Law Enforcement

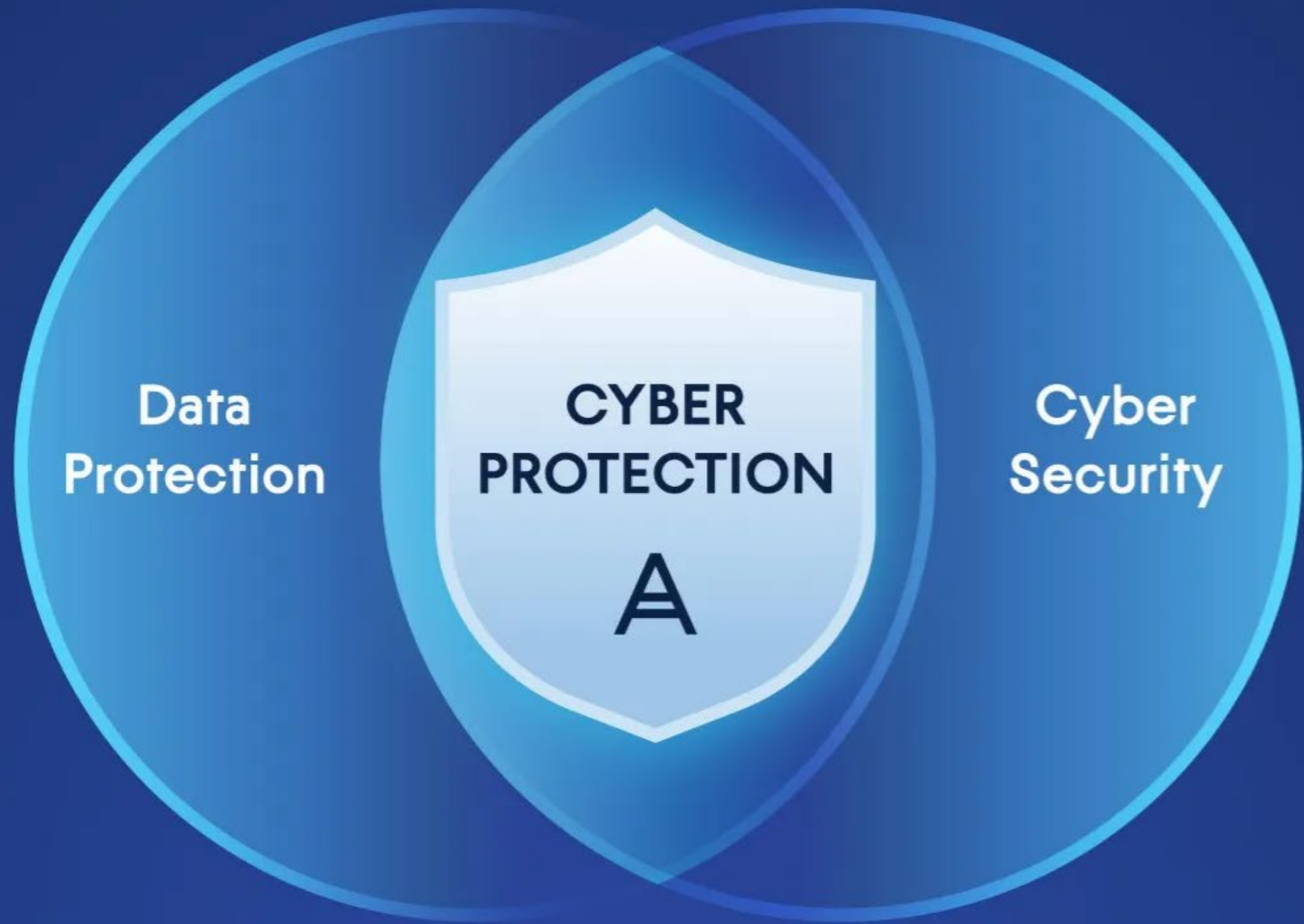
The background of the slide features three FBI officers from behind, wearing dark blue jackets with 'FBI' printed in large yellow letters. They are standing outdoors on a paved surface.

- FBI was notified
- Local law enforcement was notified

Notifications



- Notification to the staff of the incident
- Notified PII data breach and offered credit monitoring



IT Steps Taken

- Continued with Managed Detection and response (MDR) service
- Password Policy – Mandatory change two times a year
- Spear phishing campaign
- More restricted DNS Filtering

IT Steps Taken

- Multifactor Authentication
 - Email
 - Google
 - Student Information System (SIS)
 - Windows devices with access to the financial/Personnel application
 - All servers
 - Any IT applications that support MFA

IT Steps Taken

- Restricted domain admin accounts
- Further segment the network
- Geofence where supported
- Updated patch management
- Encrypt portable devices
- Frequent cybersecurity awareness message to all staff

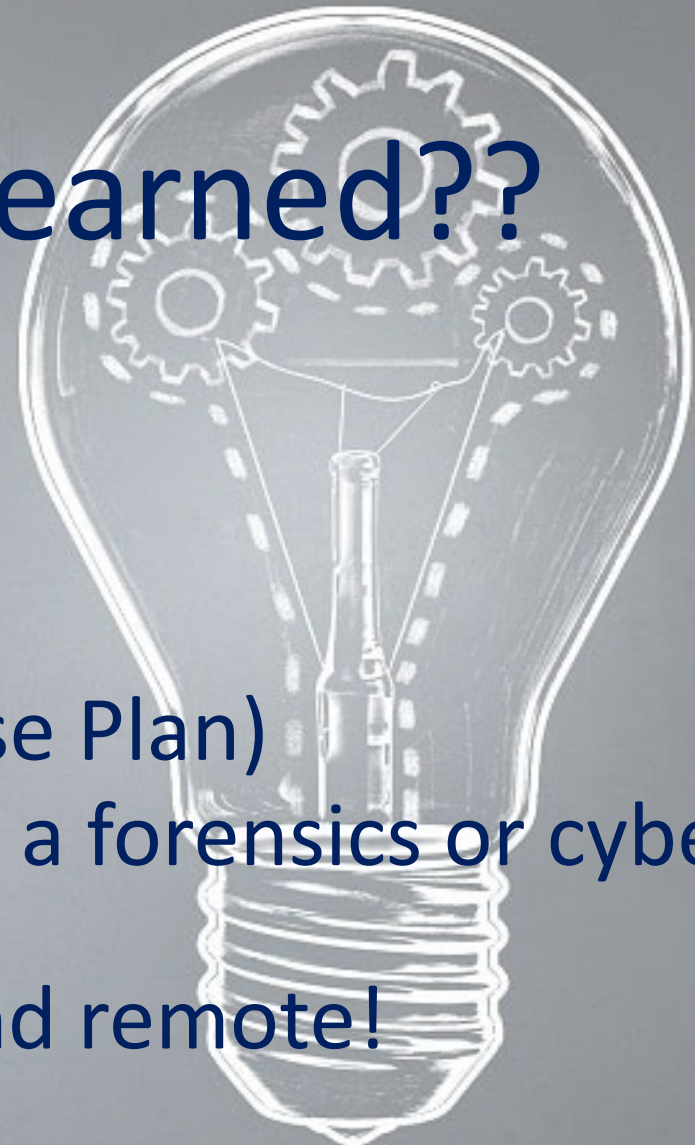
What we have learned??

- No organization too small
- Ask questions
- Communicate clearly
- Answer honestly
- Listen to experts
- Let the experts do their job



What we have learned??

- Know your risks
- Discuss your risks
- Have a good inventory
- Have an IRP (Incident Response Plan)
- Technology department is not a forensics or cyber security expert
- Have a good backup! Local and remote!



What we have learned??

Be patient!
It is a slow process!



Technology Directors

EAT
SLEEP
SHOWER
GO HOME



The background of the slide features a warm sunset scene. The sky is a gradient of light blue and orange. In the foreground, there are dark silhouettes of trees and a flagpole with a flag. The sun is visible on the right side, creating a bright glow and lens flare.

THANK YOU!

Board of Education
Superintendent
Business Administrator
Technology Staff
Everyone involved for their patience!

Q & A

