Northern Burlington County Regional School District

Breach Story

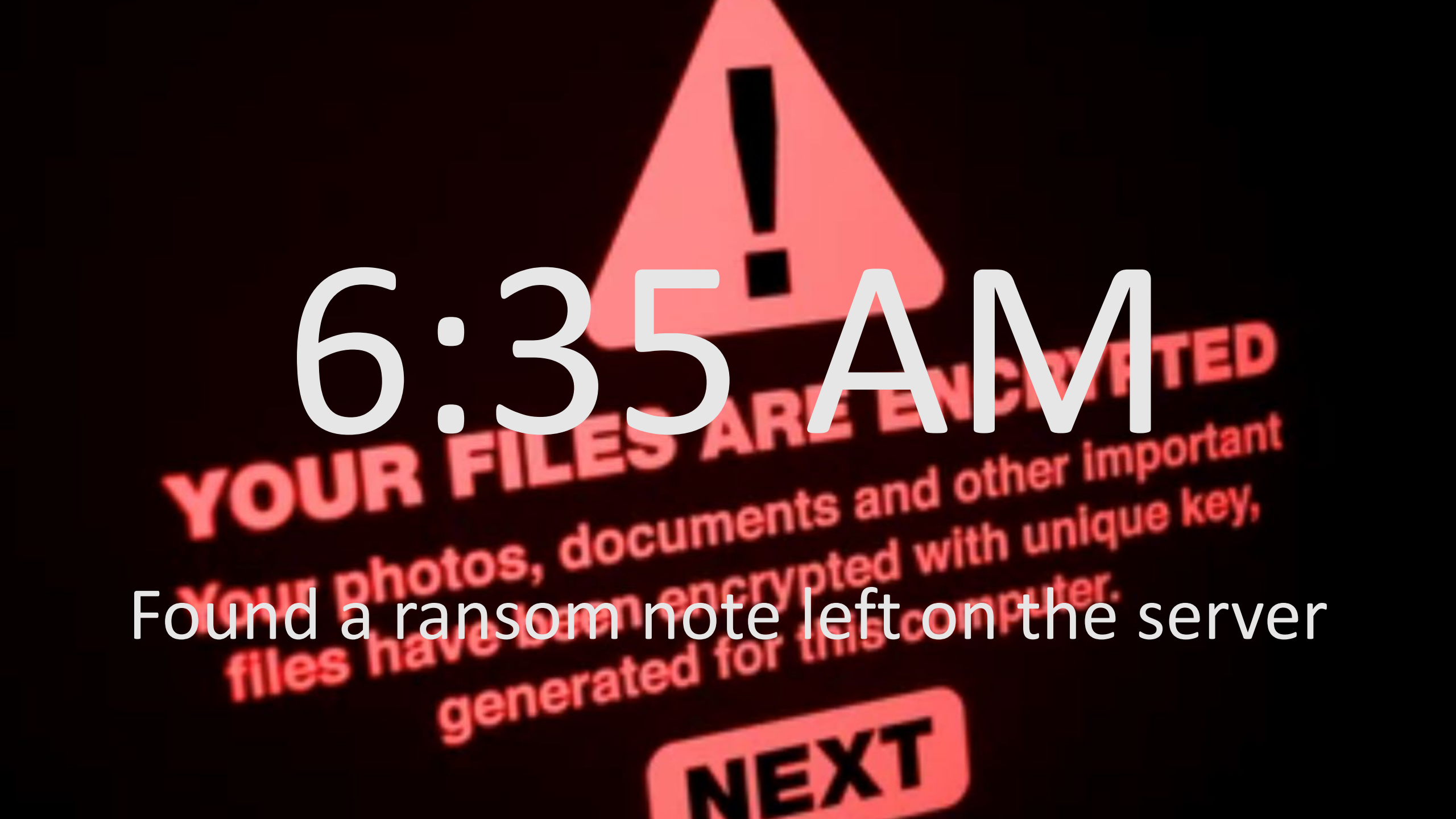
Richard Kaz, Business Administrator
Steve Lee, Director of Technology

- 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


6:30AM
Report that the transportation routing application is not functioning


6:35 AM
VPN into the application server from home to investigate
Ransomware



Found a ransom note left on the server


7:00 AM
Notified the business administrator
Ransomware


8:00AM
Business administrator notified insurance company


8:00 AM
Director of technology arrive at the district
Ransomware


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


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

- 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

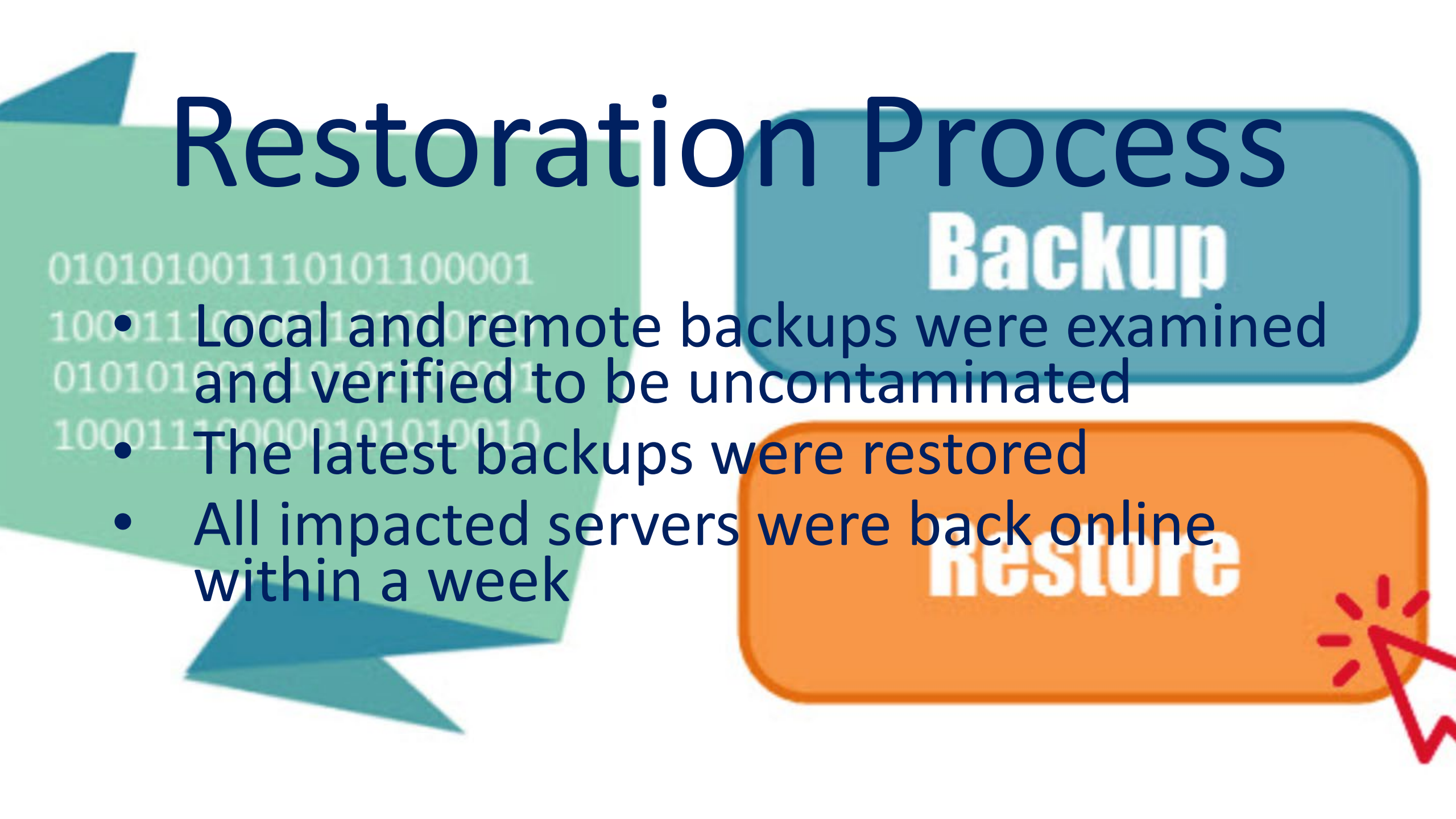
Forensic Result

Data was exfiltrated

Forensic Result

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

Restoration Process



- 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

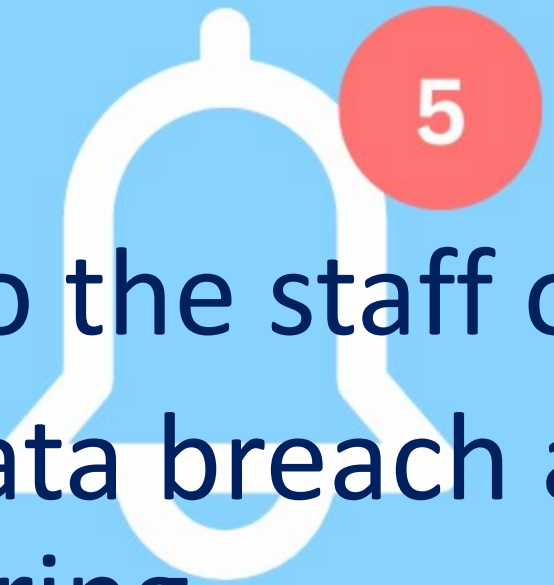
Communications

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

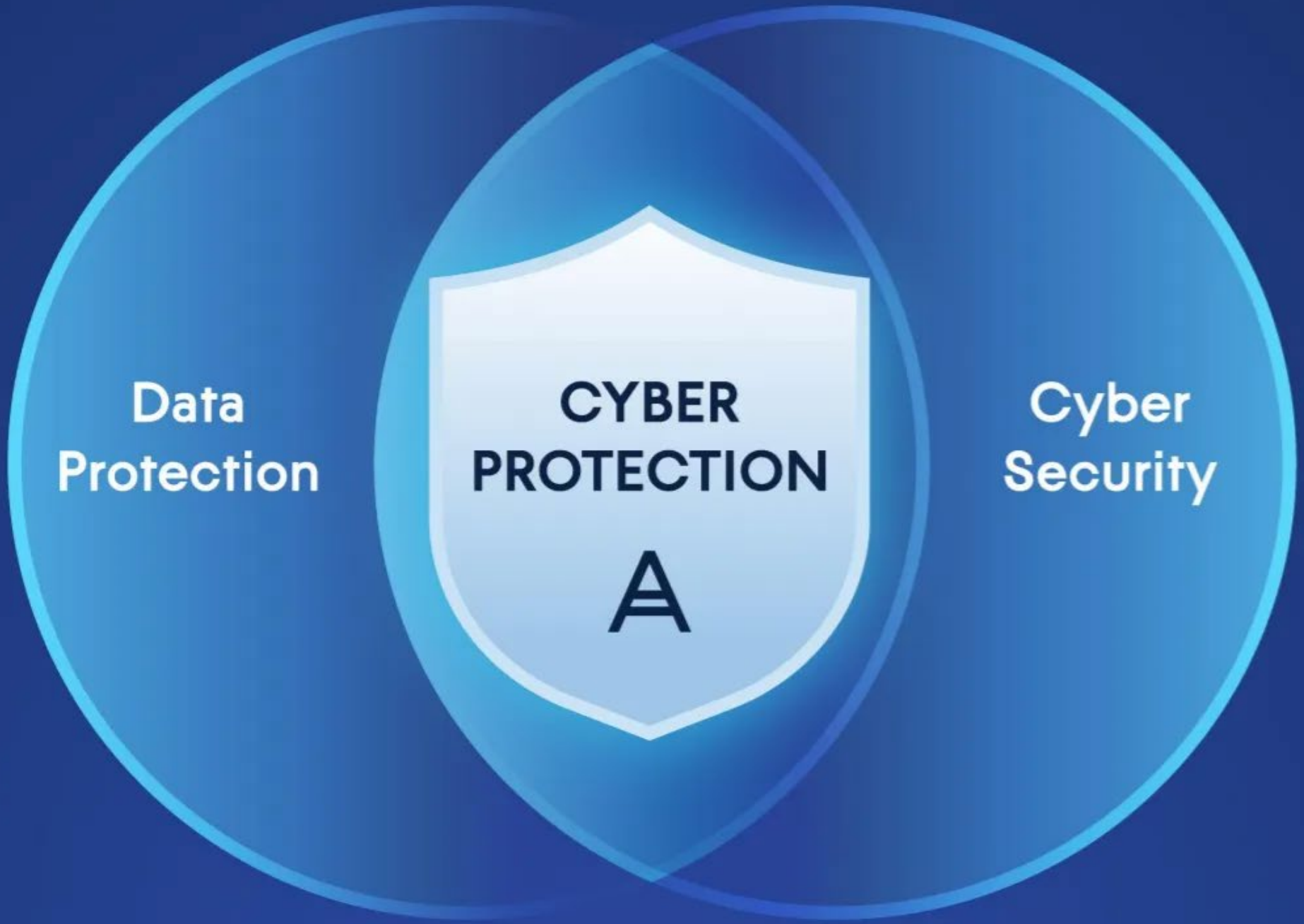
Law Enforcement

- FBI was notified
- Local law enforcement was notified

Notifications



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


Data
Protection
CYBER
PROTECTION
Cyber
Security

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

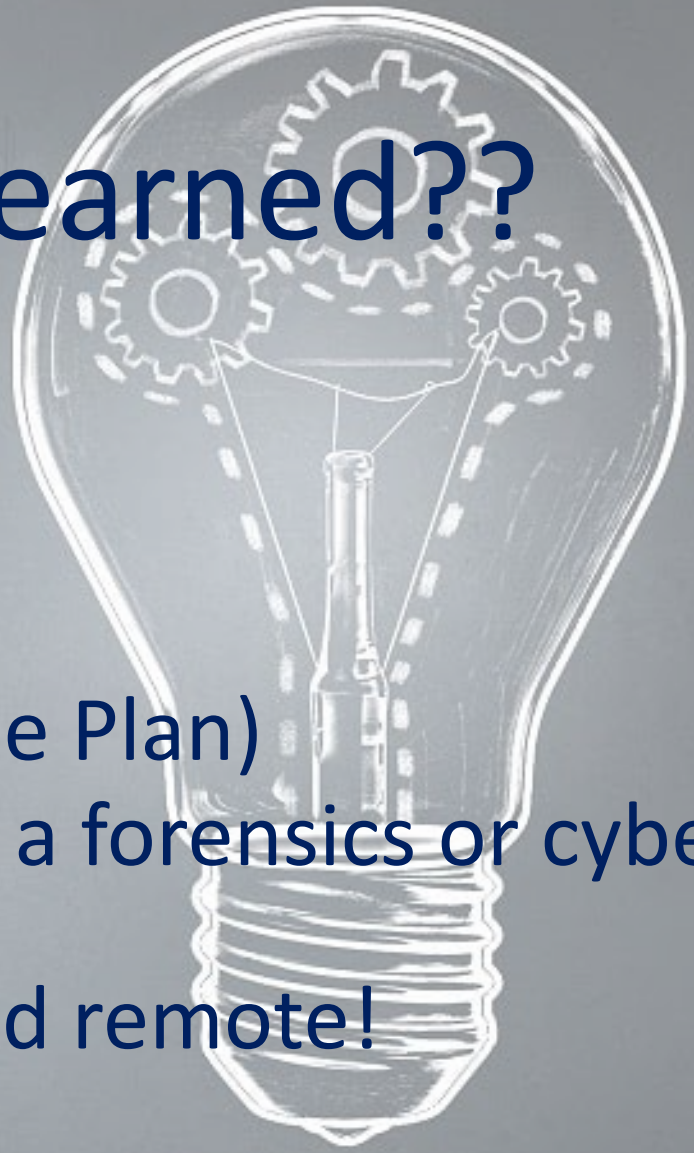
IT Steps Taken

- 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

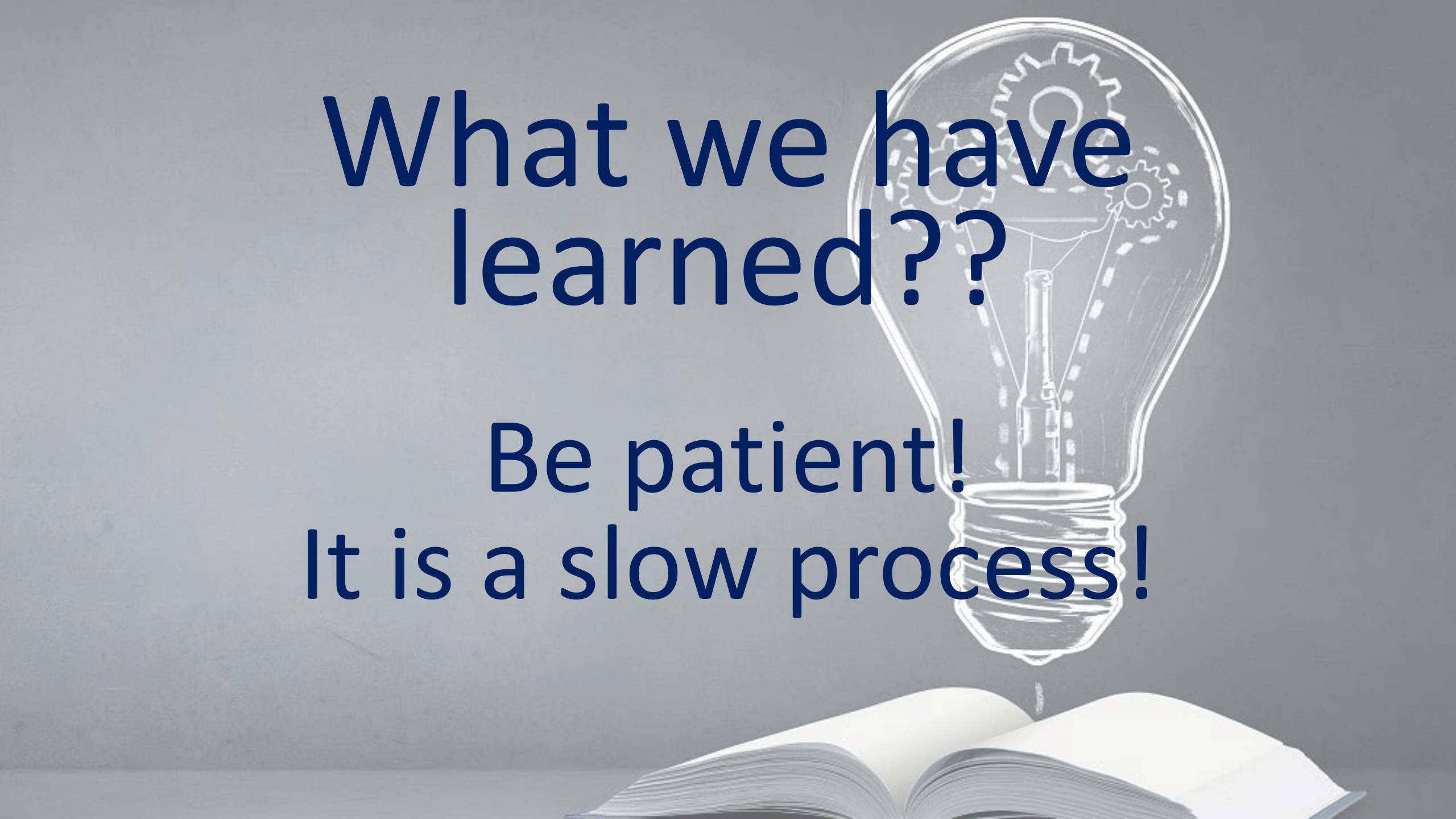
What we have learned??



- 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


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


Q&A