# Cyber Security Response

San Felipe Del Rio CISD

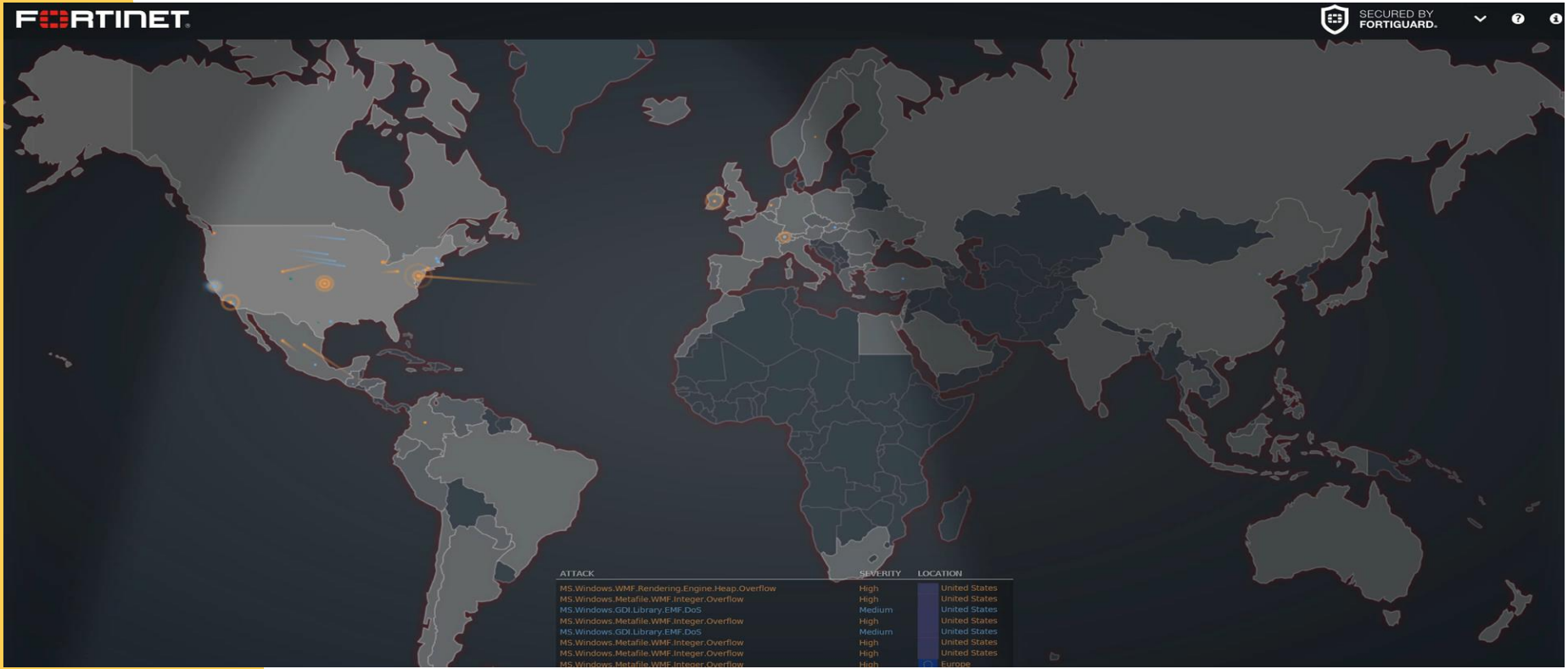
**Response Status: February 17, 2020**

**Presented By: Les Hayenga / Chief Operations Officer**

# San Felipe Del Rio CISD
# Cyber Security Protocol

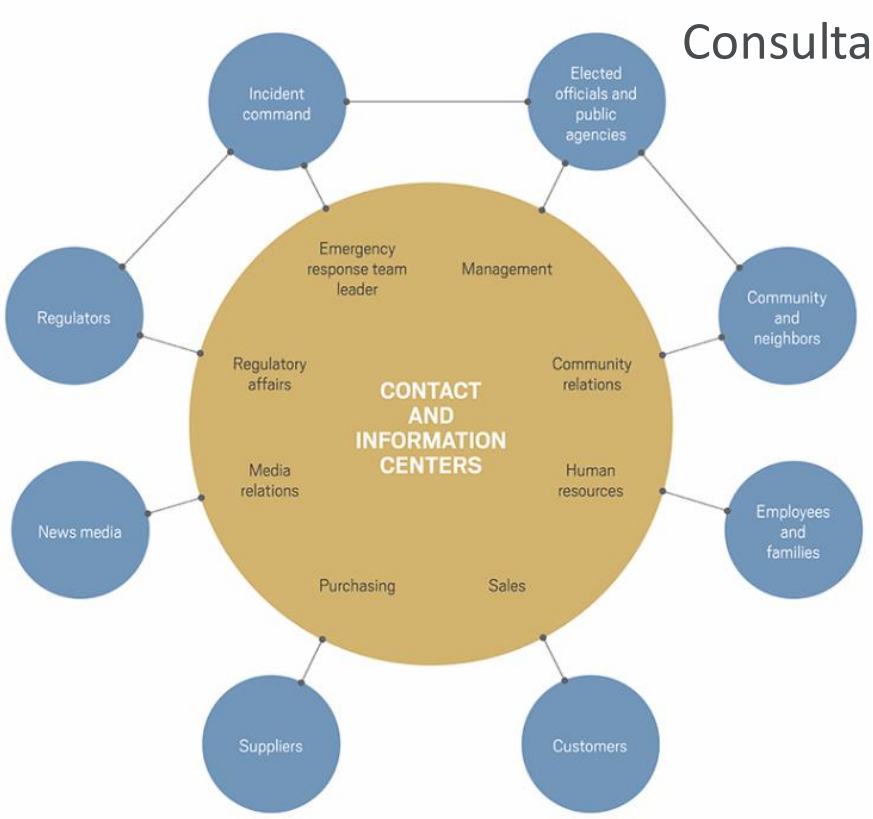
- Incident Overview
- Communication Hub
- Initial Response
- Impact to Technical Systems
- Board Policy – Emergency Procurement
- Insurance Coverage & Expenses
- After Action Review

# Incident Overview




***RYUK*** *is a high-risk ransomware-type* ***virus*** *that infiltrates systems and encrypts stored data, thereby making it unusable.*

# Communication Hub




Consultant Identified Infection

Contacted SFDR Network Administrator

1. Chief Operations Officer
2. Superintendent
3. Board of Trustees
4. Legal Department
5. Federal Bureau of Investigation
6. SFDR Public Relations
7. Texas Association of School Board
8. SFDR Staff
9. Press Release to Social Media
10. Local Media Resources

# Initial Response


- Disconnect Known Infection Area
- Identify “High Risk” Campuses
- Disconnected Campuses from Core Switches
- Dispatched Team to Assess Damage at Campuses
- Removed “High Risk” Computers from Network
- Contained and Assessed Damage at Data Center
- Began Rebuilding Critical Systems
- Cleared Campuses & Restored Internet Services
- Continue Rebuilding and Restoring Services

# Impact to Technical Systems

| Systems Not Impacted<br>Cloud Based Solutions | Systems Impacted<br>Internal Support Systems |
|---|---|
| Skyward Application | Active Directory Infrastructure |
| Microsoft Office 365 | Support Servers – Domain Controllers |
| Microsoft Cloud Storage (One-Drive) | Network File Storage – Staff & Student Folders |
| Planning Protocol Dashboard | District Printing Services |
| Instructional Applications | District Computer Labs - Virtual Desktops |
| Minimal Network Services | Internal I.T. Management Systems |
| IDPA Backup Solution (2/3 Deployed) | Estimated 300 Workstations |

# Impact to Technical Systems Continued

| Systems Still Pending | Projected Time To Restore Services |
|---|---|
| Student – V & T Drives | 10 Hours |
| Network File Storage – Staff | 20 Hours |
| Estimated 150 Workstations | 150 Hours |
| Internal I.T. Management Systems | 100 Hours |
| Total Time | 280 Hours |

# Board Policy Update

Resolution Declaring Emergency For Bidding Purposes

- Pursuant to Section 44.031(h) of the Texas Education Code in order for school personnel to correct the problem in a timely manner caused by an emergency situation, the Board must first declare that an emergency exists.

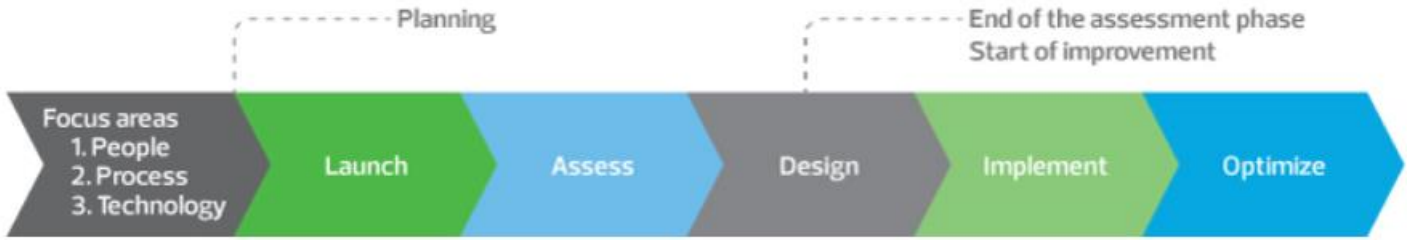

# Insurance Coverage & Expenses

The Funds Privacy & Information Security coverage provides protection for costs that members might incur in the event of a data or privacy breach and the tools needed to help resolve related issues.

- Data Breach Response – $100,000
  - Beazley Data Breach Response Services
    - Forensics, Legal Fees, and Notification Expenses

- Third Party Claims – $100,000
  - Costs incurred by TASB Approved (First Responders)
    - Weaver Technologies – Projected $30,000
    - Sequel Data Systems - $5,000

# After Action Review




The Technology Department is currently reviewing the series of events that occurred, and will have recommendations in the upcoming weeks.

# Questions