Jackson County ISD Ransomware Attack - Frequently Asked Questions

Incident Overview

1. **What happened?**
   Jackson County Intermediate School District suffered a ransomware attack that affected critical operating systems in the district. Immediately upon discovering suspicious activity, we proactively took systems offline in order to contain the incident. External cybersecurity advisors have been engaged to investigate and assist in the safe restoration of our systems. We have also notified law enforcement and are cooperating in their investigation.

2. **Are all systems back online?**
   At this time, our essential systems are safely up and running for use by teachers, staff, students, and parents, while certain supplementary systems are actively being restored.

3. **Is the threat contained?**
   Yes. To date, we have no evidence to suggest our systems are still at risk. Our essential systems are safely up and running for use by teachers, staff, students, and parents, while certain supplementary systems are actively being restored.

4. **Is it safe to return?**
   Yes, it is safe for our students to return back to school. While our recovery efforts continue, we prioritized bringing essential systems back online in order to allow us to safely resume operations and reopen school buildings across Jackson and Hillsdale counties.

5. **Was it really necessary to take the children out of school for multiple days?**
   Yes. In addition to our online portals, our telephone systems and HVAC systems were also impacted, which presented an unsafe environment for our students.

6. **How do the days off affect the school year?**
   Jackson County ISD will count Monday, November 14, 2022 – Wednesday, November 16, 2022, as Act of God Days. These days are proactively built into the school year and prevent unforeseen school cancellations from elongating the academic school year.

7. **What steps were taken to secure the environment?**
   Immediately upon discovering suspicious activity, we proactively took systems offline in order to contain the incident. We have engaged external cybersecurity advisors to investigate and assist in the safe restoration of our systems. We have also notified law enforcement.

Data & Investigation

8. **Are the criminals responsible for this attack targeting our children?**
   We have no evidence to suggest any individual was the target of this attack. Ransomware attacks such as these are typically opportunistic crimes in search of financial gain.

9. **Why can't we have more details about the attack?**
   The investigation into this incident is ongoing and investigations of this nature may take some time. We are committed to sharing updates with you as necessary as the investigation progresses.

10. **Is my or my child’s data at risk?**
    Our technology team is currently working alongside third-party cybersecurity experts to investigate the scope of this incident. If we determine sensitive data may have been affected as the result of this incident, we will notify individuals in accordance with our obligations.

11. **How long will this investigation take?**
    Our investigation is ongoing. Our technology team is currently working alongside third-party cybersecurity experts to investigate the scope of this incident, and they are doing everything in their power to conduct this investigation quickly and thoroughly. Investigations like these can take time and we will provide more information as it becomes available.

What Happens Next

12. **Where do I go if I have additional questions?**
    At this time, we do not have any additional information to provide. We are committed to sharing updates with you as necessary as the investigation progresses.

13. **Is there anything I should do to further protect myself?**
    We encourage everyone to use standard cybersecurity best practices including frequently changing your passwords, having different passwords across your personal and professional logins, and not opening emails from people and businesses you are not familiar with.

    There are also steps you can take to be vigilant against any potential incidents of identity theft and fraud. You can review your credit reports, as well as credit card, bank, and other financial statements for any unauthorized activity. If you notice any unauthorized activity, contact the relevant financial institution or the credit bureau reporting the activity immediately.

14. **How will you make sure this doesn't happen again?**
    Unfortunately, ransomware attacks targeting public school systems such as the one we faced are on the rise. However, we are dedicated to safeguarding the data we hold within our systems. Our investigation into this matter is ongoing and we will provide more information as it becomes available.