BEST PRACTICES

CYBER SECURITY

According to Homeland Security, cyberattacks were up over 300% last year. That means it is more important than ever to ensure your district invests in appropriate cyber security including training, enhanced security systems, monitoring, updated incident response plan, and appropriate cyber coverage for when something does happen.

Below are some best practices learned from a massive ransomware attack at a member district.

FACTS OF THE CYBER ATTACK: An email with a malicious attachment was sent to employees of the district; an employee opened the attachment and unknowingly allowed a hacker into the district system. For three days, the hacker was in the district system. After business hours on the third day, a Friday in this case, the ransomware attack came, infecting 300 servers and 400 workstations. The affected data and key systems were backed up regularly on tape backups, but even some backup systems were breached. Although the cyber response was enacted on Saturday morning, operations were impacted at all school and district sites on Monday including email, internet access, transportation routing info, accessing student records, and curriculum software. The key systems were restored within a few weeks through the use of tape backups, but all systems were not fully operational for approximately 4 months.

WHAT IS RANSOMWARE: Ransomware is a form of malware in which software code infiltrates a computer through open security vulnerabilities and essentially encrypts a user's computer (or a district's entire system) and holds the data hostage until a ransom is paid.

INCIDENT RESPONSE: With a flood of alerts overnight, the IT team went onsite to troubleshoot and immediately called the risk manager when a ransom note was found alongside encrypted files and systems. The risk manager engaged with Beazley, the cyber coverage provider offered through CSRM, and notified the Superintendent and Cabinet. With Beazley notified within 24 hours of discovery, the district was able to sign contracts with vetted and available resources to evaluate exposure and damages, negotiate with the bad actor, communicate with current school principals and staff, and prioritize and restore key systems. Risk management engaged with school safety who established an Emergency Operations Center who coordinated with FBI, DHS, and local law enforcement.

BEST PRACTICES AND LESSONS LEARNED:

- Many ransomware attacks happen similarly to this, with the bad actor waiting until after hours when they suspect no one will be around to stop the

attack swiftly. Increasing the monitoring of actionable system alerts can help a district respond more quickly and help contain the attack.

- Assess endpoint protections including checking alerts and monitoring vulnerabilities. Beazley has partners that provide endpoint protection software and can be used in an on-going basis to help closely monitor vulnerabilities and make efforts to contain them.

- Educate and provide regular training to end users about cyber security. Conducting phishing email tests to see if users click on malicious looking emails and educating those who do.

- Tape backups for this district meant a delay in discovery and made restoration of systems difficult. Using a disc or cloud-based backup system could prevent a delay and make restoration of key systems less challenging. Make sure to test the district backup system on a regular basis. The system should be immutable to cyber or ransomware attacks, and should fall within your district's threshold RTO (recovery time objective).

- Have an updated cyber incident response plan. This response plan should include steps to take when different types of incidents occur (ransomware, virus, etc.) as well as a communications plan for when email and other communications systems are down. This should also include a prioritized list of key systems so that IT can begin restoring the most critical systems first.

- Invest in your cyber security. This includes acquiring updated backup systems, diversifying network systems, and working with risk management for appropriate cyber coverage should a cyber attack occur.

- Ensure that all contracts with any software or network providers include hold harmless and indemnification language because many will not automatically include that policy language.

The best practices and lessons learned above are not intended to be exhaustive, but should provide basic guidance for your district. For more information or if you have any questions, please contact your California Schools JPA risk manager at 909-763-4900.