



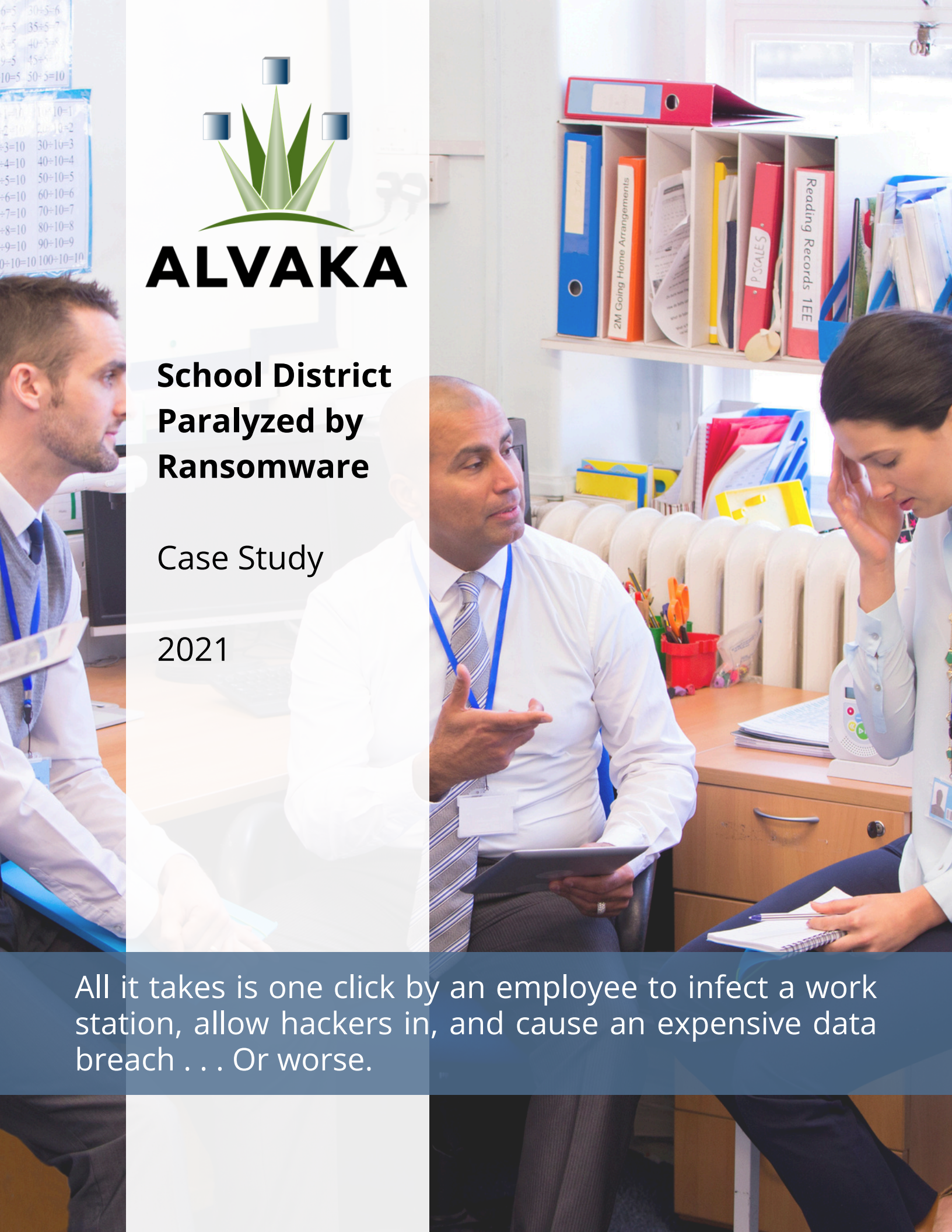
ALVAKA

**School District
Paralyzed by
Ransomware**

Case Study

2021

All it takes is one click by an employee to infect a work station, allow hackers in, and cause an expensive data breach . . . Or worse.



OVERVIEW

Initial Complications

A group of cybercriminals used ransomware to disrupt the operations of a school district that comprised of over 10,000 students. Both students and staff were unable to access their workstations, and a multi-million dollar ransom was demanded. A global incident response firm (IR), who was notified by the school district, began their IT forensics and incident response. Soon after, a communication line was established between IR and the threat actors to start the process of negotiating a discounted ransom.

Beginning of the Recovery Process

Meanwhile, the internal IT staff was asked to perform remediation tasks to support the recovery process. They also deployed software agents to lock out threat actors. Restoring critical applications such as payroll and email, combined with the effort of negotiating and restoring workstations, overwhelmed the IT staff. After ten days, the school district and IR decided to contact Alvaka to relieve the workload on internal IT staff.

CHALLENGES

Due to the extent of the attack, students were unable to perform mandatory state testing, and the ability to remotely access e-learning was impeded. Other integral applications such as email, web servers, and documents ceased to function. Consequently, teachers were incapable of accessing essential student curriculum, and classroom operations were hindered. Additionally, the lack of centralized management in the network environment produced a laborious restoration process.

RESULT

After successful recovery of all networks and workstations, the district was able to avoid paying the multi-million ransom. Alvaka's services allowed the district to become operational and enable students to return to class. Additionally, the district was able to implement proper security measures for their network that were not in place prior to the incident.

ABOUT US

Alvaka manages and secures the IT infrastructure of mid-market and enterprise-class companies. Alvaka specializes in providing rapid response ransomware recovery services, aiding companies in returning to normalcy swiftly post-breach. Our 24x7 live support, 365 days a year, is delivered by a dedicated US-based staff.

Alvaka has enjoyed over four decades working in partnership with our clients, and we remain committed to our purpose of improving their lives through our IT management and security services.

Learn more about Alvaka at www.alvaka.net.



(949) 428-5000

sales@alvaka.net

