atRISK Technologies

CUSTOMER USE CASE

Independent School District

INDUSTRY

- Education
- Nonprofit

CHALLENGE

- Detecting novel attacks and insider threats at an early stage
- Imperative to protect students' personal information
- A need to comply with increased regulatory requirements, including FERPA & PPRA

RESULTS

- Deployed the atRisk Technologies Quorum Platform
- Provided Cybersecurity Roadmap to mitigate network risks
- Cybersecurity training provided to District's Information Technology and Security staff
- Gained real-time security insights necessary for regulatory compliance

Public school districts are a new favorite target of cybersecurity attacks.

Due to the wealth of data and limited budgets for cybersecurity training, software solutions and staff, schools have drawn the attention of hackers. Ransomware and Phishing attacks are now being directed at school districts across the country.

In July 2019 alone, cyberattacks hit systems in Arizona, New Mexico, Nevada, Louisiana, Oklahoma, Alabama, Connecticut, and New York. Such attacks are continuing to occur and show no signs of ceasing.

Regrettably, I.T. staff at schools and districts often only have access to disparate cybersecurity tools, outdated software, and lack the expertise of trained cybersecurity professionals.

Cybercriminals easily employ targeted attacks that result in high financial costs, personal information violations or negatively impact a district's reputation.

> With atRisk Technologies, I was amazed at how much network insight I gained.
>
> SR. DIRECTOR OF RISK MANAGEMENT AT A LARGE TEXAS ISD

CHALLENGE

Today's educational systems collect and store substantial amounts of confidential personal information of both students and staff. They are also often networked across government network systems. This data and connectivity attract the world's most sophisticated criminals, where these institutions often have gaps in their cybersecurity defenses.

Recently a Texas public school district's insurance broker made a call to the District's Risk Management Office, inquiring about possible security gaps the District may be facing. The Risk Management office is responsible for ensuring the cybersecurity and risk management of 12,000 employees and 86,000 students. The broker attended an educational seminar hosted by atRisk Technologies, which brought to light the fact that many organizations have technology gaps that need attention, and most have understaffed I.T. departments that cannot address threats as they occur. The Sr. Director of the Risk Management Office, acknowledged that their current technology stack contains holes and they needed to improve overall visibility into the network.

The Sr. I.T. Director's greatest fear was an issue or event that would be missed by the overburdened staff that would result in either a severe breach of the network or have them become a victim of a targeted ransomware or malware attack. There was a vital need to ensure the District's cybersecurity posture was hardened, and the I.T. office was performing proactively instead of reactively. The goal was to quickly change from 'not knowing what they did not know' to a more definitive state.

Finally, the District did not believe its current security tools were sufficient to comply with the regulatory requirements on data protection laid out by the mandates of The Family Education Rights and Privacy Act (FERPA), and the newly enacted Texas Legislative Bill S.B. 820. By law, the District is required to ***adopt a cybersecurity policy to secure the District's cyberinfrastructure against cyber-attacks and other cybersecurity incidents, and the implementation of a security incident plan had to be put in action.***

SOLUTION

Following the completion of a successful Proof of Value (POV) trial, the school district deployed atRisk Technologies' platform Quorum. The platform quickly established the District's baseline security posture along with health scores and provided an actionable road map for improvement.

atRisk Technologies provided the District's Risk Management Office the ability to understand what cybersecurity risks threatened the environment. Through routine meetings, touchpoints, and reports provided by the atRisk's ACE Services Team, the District's I.T. and security operations teams became educated in the art of cybersecurity defense. A customized dashboard provided an aggregated, analyzed, and unified view of data across devices, apps, users, networks, and other security products. The District's I.T. team are able to execute on actionable insights and achieve their goal of being in a proactive state rather than a reactive one.

BENFITS

The Quorum platform proved to be a game changer for the school district's technology and security teams, allowing for gap analysis of their technology and processes. Providing a reduction of overhead costs and personnel exhaustion from multiple dashboards through Quorum's single, unified interface. Today the District has achieved a deep understanding of the full sequence of events leading up to a security incident.

> "I no longer stay up at night worrying about when or how we will be breached, or if we will be the next victim of a malware or ransomware attack."
>
> **SR. DIRECTOR OF RISK MANAGEMENT AT A LARGE TEXAS ISD**

LEARN MORE OR ARRANGE A DEMO AT INFO@ATRISK.COM.

@RISK
TECHNOLOGIES

16400 Dallas Pkwy.
Suite 100
Dallas, TX 75248

+1-800-426-0178
info@atrisktech.com
www.atrisk.com