School cyberattacks disrupt learning, divert student resources, and subject victims and districts alike to costly recovery efforts. Texas law requires school districts to implement a cybersecurity plan designed to protect against and recover from breaches.

Santa Anna ISD names Larry Bostick as the district Cybersecurity Officer. Furthermore, SAISD will continually develop and implement cybersecurity policies to keep the district, it's employees, staff, and students safe from cyberattacks and breaches.

Cybersecurity Framework

Functional Area	Description
Identify 	Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
Protect 	Develop and implement appropriate safeguards to ensure delivery of critical services.
Detect 	Develop and implement appropriate activities to detect the occurrence of a cybersecurity event.
Respond 	Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
Recover 	Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

The framework, which is aligned with the National Institute of Standards and Technology (NIST) framework, is divided into five concurrent and continuous functions: Identify, Protect, Detect, Respond, and Recover. Each functional area contains specific security control objectives to help organizations identify, assess, and manage cybersecurity risks in their environment.