Managed Methods

CyberDefense Playbook

Secure Google & Microsoft with Limited Resources

Presenter

Tom Schmidt

Senior Account Executive - Texas

Managed
Methods

Presenter

Corey Anderson

Technology Director - Maypearl ISD

Managed Methods

Agenda

1. Introduction
2. Why Investigations & Audits Are Important
3. 5 Critical Investigations & Audits
4. Q&A

Based in Boulder, Colorado since 2014

Dedicated customer success & support team

40+ employees focused on education

Parents with children in schools

Google for Education Partner

Google Cloud Partner

Microsoft Partner Education Specialist

Student Data Privacy Consortium

ACPE NORTHWEST

CoSN LEADING EDUCATION INNOVATION

Cybersecurity, Student Safety, and Compliance Made Easy

From the browser to the cloud, **ManagedMethods provides easy, affordable cybersecurity and student safety monitoring** in school-provided technology to technology leaders who need to secure online learning on a tight budget

Managed Methods

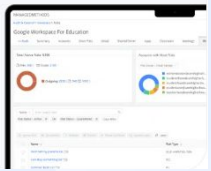
Managed Methods

Easy and affordable **cybersecurity, student safety, and classroom engagement tools** engineered specifically for K-12 schools

Cloud Monitor

Cloud Monitor makes Google Workspace and Microsoft 365 cloud security and safety easy for K-12 schools – no proxy, no agent, no extension, and no special training required.

Learn More



Content Filter

Content Filter is a cloud-based web filtering solution designed to help schools block harmful, inappropriate, and distracting online content while enabling safe access to educational resources.

Learn More

Classroom Manager

Classroom Manager is a browser-extension-based classroom management tool designed to make online instruction and learning more effective for teachers and students.

Learn More

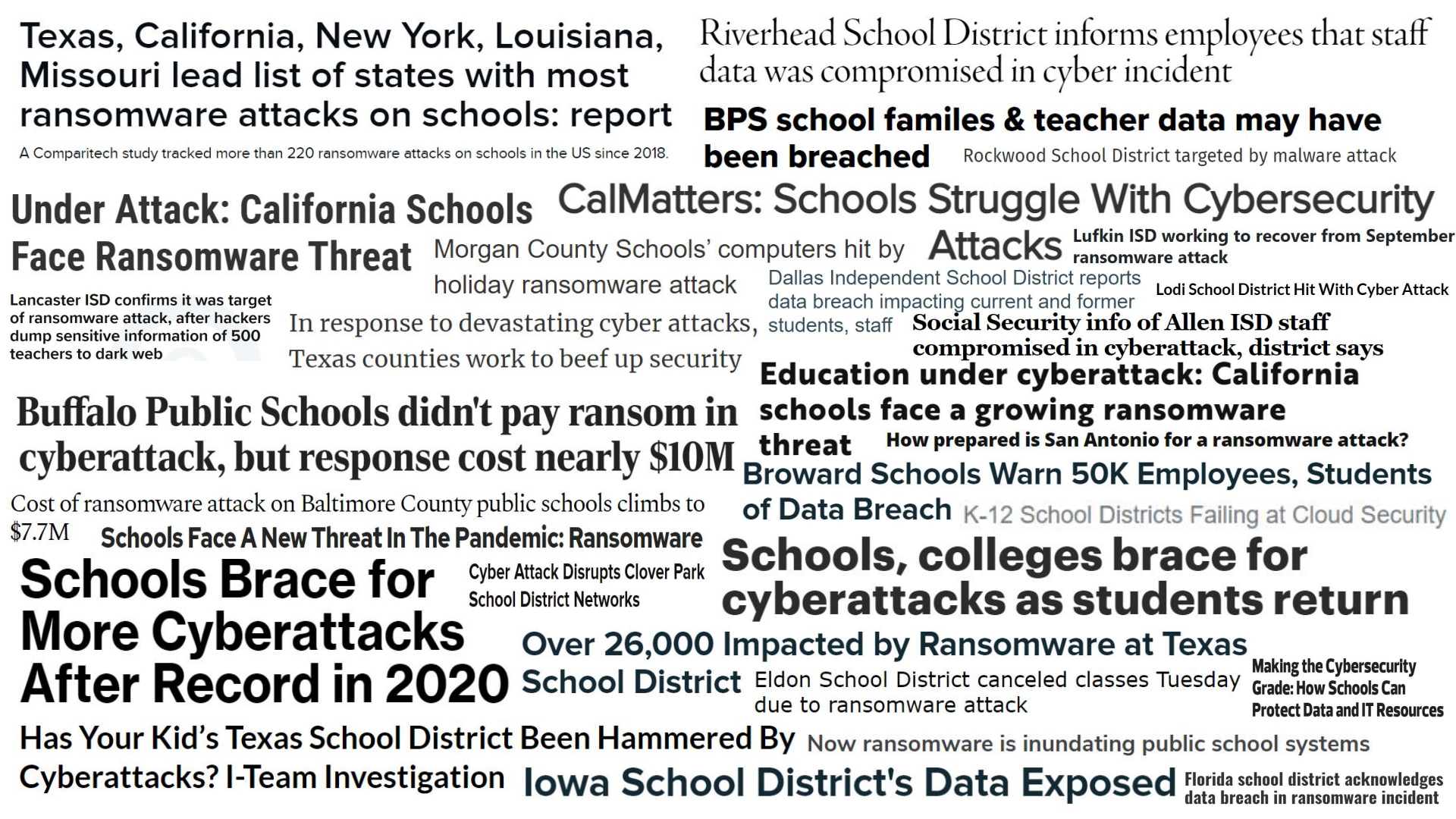
The Problem

- 52% of US districts experienced a cybersecurity incident in 2025. 36% increase from 2024.
- 3rd Party Incidents Highlight the Reality of Shared Risk. 28% increase from ‘24 to ‘25
- Student Identity theft is now the #1 concern for 54% of US districts. Yet districts less than 21% of all districts deploy a cloud data loss prevention or monitoring system.
- A.I. is amplifying risk faster than schools can respond.

Managed Methods

Why Investigations & Audits Are Important

Managed Methods


Texas, California, New York, Louisiana, Missouri lead list of states with most ransomware attacks on schools: report
A Comparitech study tracked more than 220 ransomware attacks on schools in the US since 2018.
Riverhead School District informs employees that staff data was compromised in cyber incident
BPS school familes & teacher data may have been breached
Rockwood School District targeted by malware attack
Under Attack: California Schools Face Ransomware Threat
Lancaster ISD confirms it was target of ransomware attack, after hackers dump sensitive information of 500 teachers to dark web
CalMatters: Schools Struggle With Cybersecurity Attacks
Morgan County Schools' computers hit by holiday ransomware attack
Lufkin ISD working to recover from September ransomware attack
Dallas Independent School District reports data breach impacting current and former students, staff
Lodi School District Hit With Cyber Attack
In response to devastating cyber attacks, Texas counties work to beef up security
Social Security info of Allen ISD staff compromised in cyberattack, district says
Education under cyberattack: California schools face a growing ransomware threat
How prepared is San Antonio for a ransomware attack?
Buffalo Public Schools didn't pay ransom in cyberattack, but response cost nearly $10M
Broward Schools Warn 50K Employees, Students of Data Breach
K-12 School Districts Failing at Cloud Security
Cost of ransomware attack on Baltimore County public schools climbs to $7.7M
Schools Face A New Threat In The Pandemic: Ransomware
Schools Brace for More Cyberattacks After Record in 2020
Cyber Attack Disrupts Clover Park School District Networks
Schools, colleges brace for cyberattacks as students return
Over 26,000 Impacted by Ransomware at Texas School District
Eldon School District canceled classes Tuesday due to ransomware attack
Making the Cybersecurity Grade: How Schools Can Protect Data and IT Resources
Has Your Kid's Texas School District Been Hammered By Cyberattacks? I-Team Investigation
Now ransomware is inundating public school systems
Iowa School District's Data Exposed
Florida school district acknowledges data breach in ransomware incident

Districts Need Multi-layered Cybersecurity & Safety

Cloud	Email (Gmail or Outlook & MS Exchange Online) File Sharing (Drive, Shared Drives, OneDrive, Sharepoint) Video Conferencing / Messaging (Meet, Chat, Teams, Zoom)
Identity & Access	MFA / 2FA SSO
Endpoint	Content Filtering (CIPA / E-Rate) Virus Protection (PCs and & Mac) Classroom / Device Management (MDM)
Network	Firewall Secure Wifi Network Content Filtering
Infrastructure	Vulnerability / Pen Testing Remote Access (VPN) Patch Management (Windows) Backup

Managed Methods

Managed Methods

What is a Security & Safety Audit?

A periodic inspection of security risks in your district's Google Workspace, Microsoft 365, and online browsing content and behaviors. Common risks include:

- "Shadow" 3rd party applications
- Non-compliant sharing of PII, PCI, IEP, health information, etc
- Copyright protected file sharing (ex: movies)
- Compromised accounts
- Phishing in email & shared files
- Which accounts are using VPNs
- Sexual, violent, and otherwise inappropriate content
- And much more...

Managed Methods

5 Critical Investigations & Audits to Protect Your District

Managed Methods

Investigation #1

3rd Party Apps

- Are users connecting inappropriate and/or risky apps to my domain?
- Are app permissions overly broad?
- Are connected apps compliant with student data privacy laws?

Investigate 3rd Party Apps in Google

Investigate 3rd Party Apps in Microsoft 365

Investigate 3rd Party Apps in Cloud Monitor

Managed Methods

Investigation #2

Suspicious Login Activity

- Am I able to identify account logins from untrusted countries or regions?
- Can I see patterns of user behavior which might indicate a compromised account?
- Can you identify which students are using VPNs to log in to their accounts?

Investigate Login Activity in Google

Investigate Login Activity in Microsoft 365

Investigate Login Activity in Cloud Monitor

Managed Methods

Investigation #3

Drive Files & Sharing

- Are files containing PII, financial information, etc. being shared inappropriately?
- Are there any files containing malware in my user's drive files?
- Are students/teachers uploading movies and other copyrighted material?

Investigate Drive Files & Sharing in Google

Investigate Drive Files & Sharing in Microsoft 365

Investigate Drive Files & Sharing in Cloud Monitor

Managed Methods

Quick Wins

HTML Games stored in Drive

Managed Methods

Investigation #4

Safety Signals

- Are students sharing inappropriate, explicit, violent content?
- Are shared docs, slides, etc. being used for cyberbullying?
- Are students discussing self-harm, suicide, or other concerning behaviors?
- Are students inappropriately communicating outside my domain?

Investigate Safety Risks in Google

Investigate Safety Risks in Microsoft 365

Investigate Safety Risks in Cloud Monitor

Managed Methods

Investigation #5

Risky Emails

- Are users sending PII, credit cards, W2s, etc. via email?
- Are phishing emails coming into the domain?
- Are phishing emails being sent within my domain?
- Are students sending inappropriate emails?

Investigate Risky Emails in Google

Investigate Risky Emails in Microsoft 365

Investigate Risky Emails in Cloud Monitor

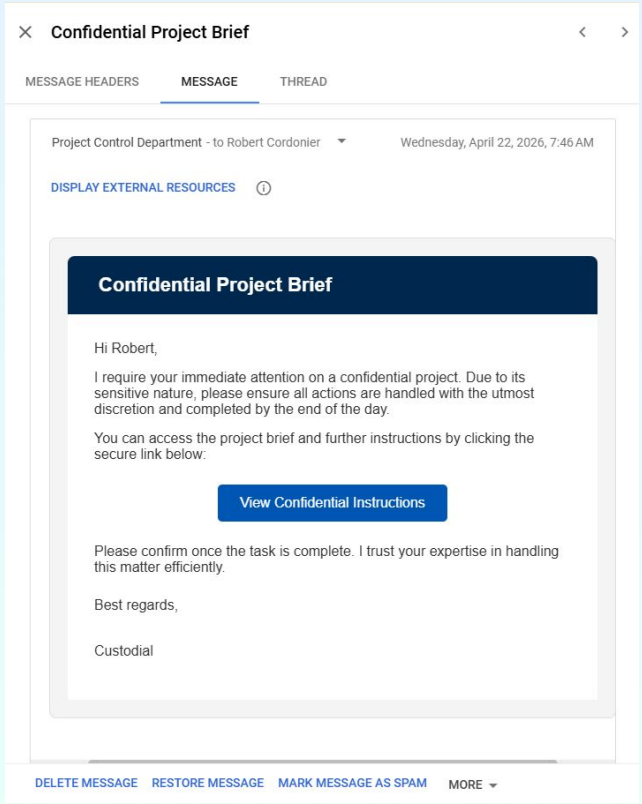
Managed Methods

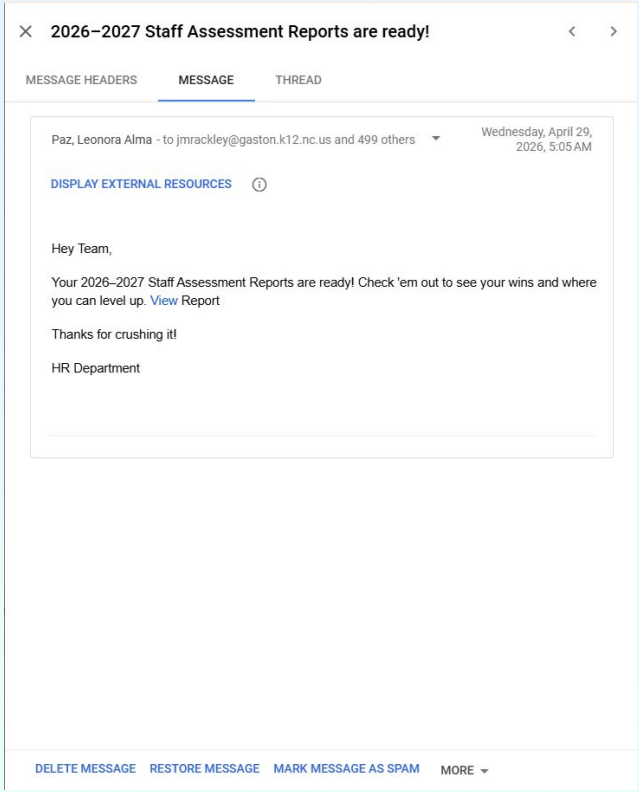
Quick Wins

Phishing Emails

Managed Methods

Phishing Emails





Managed Methods

Advanced Phishing Models are trained on these:

Mismatched Senders & Domains
Key red flags indicating illegitimacy.

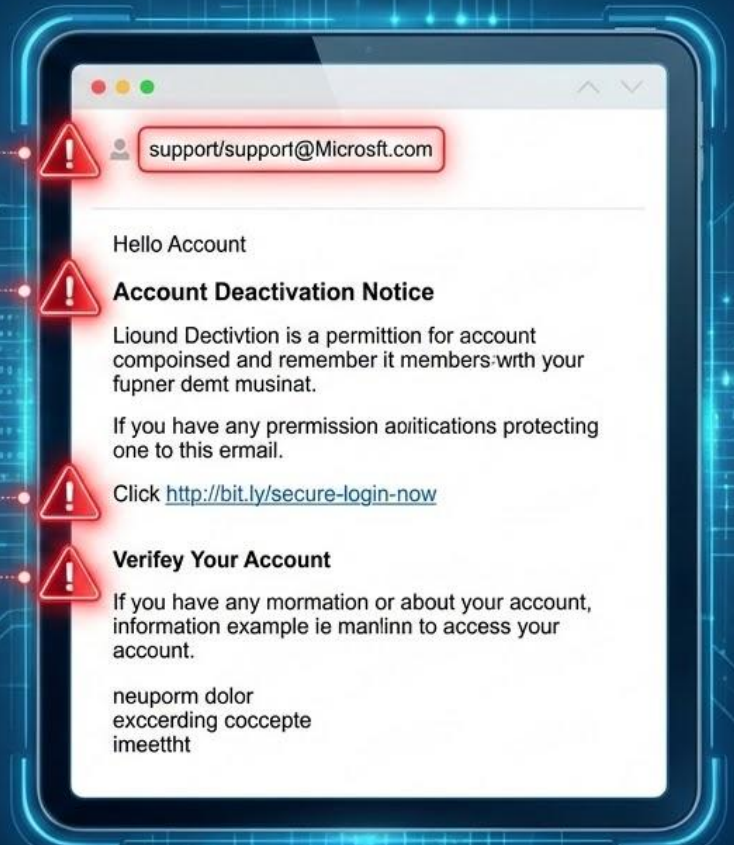
Urgency & Threats
Pressure tactics to force hasty action.

Impersonating Leadership
Faking authority figures to gain trust.

Suspicious Links, QR Codes
Malicious URLs and codes leading to fake sites.

Unusual Financial Requests
Unexpected demands for payment or data.

Odd Attachments or Instructions
Files or steps that deviate from normal procedures.



BONUS!

Automate Investigations

- Do I have time to run all of these investigations manually?
- Do I have the time and resources to monitor for address incidents as they arise?
- Are there incidents that I need to prioritize over others?

Automate Investigations in Google

Automate Investigations in Microsoft 365

Automate Investigations in Cloud Monitor

Managed Methods

Managed Methods

Why Schools Partner With Us

User Experience

Single platform for Google, Microsoft & Zoom

Triage & solve problems faster

Intuitive, easier to use and more efficient

No security expertise required - IT pros, principals & counselors all benefit

Visibility & Control

More granularity in Google Workspace & Microsoft 365

3rd party apps

Live file & email search

Account identity & access

Powerful DLP

Student Safety Signals

Advanced machine learning & artificial intelligence

Detect self-harm, cyberbullying, threats of violence, sexual content

Role-based notifications route alerts to schools directly and the staff trained to address

Thank You!

Cybersecurity
Text & Image Risks

- Student Data Privacy
- Data Loss Prevention
- Financial Data Security
- HR/Employee Data Security
- Phishing & Malware Protection

Student Safety
Text & Image Risks

- Self Harm
- Cyberbullying
- Domestic Abuse
- Threats of Violence
- Explicit Content

Managed Methods

managedmethods.com