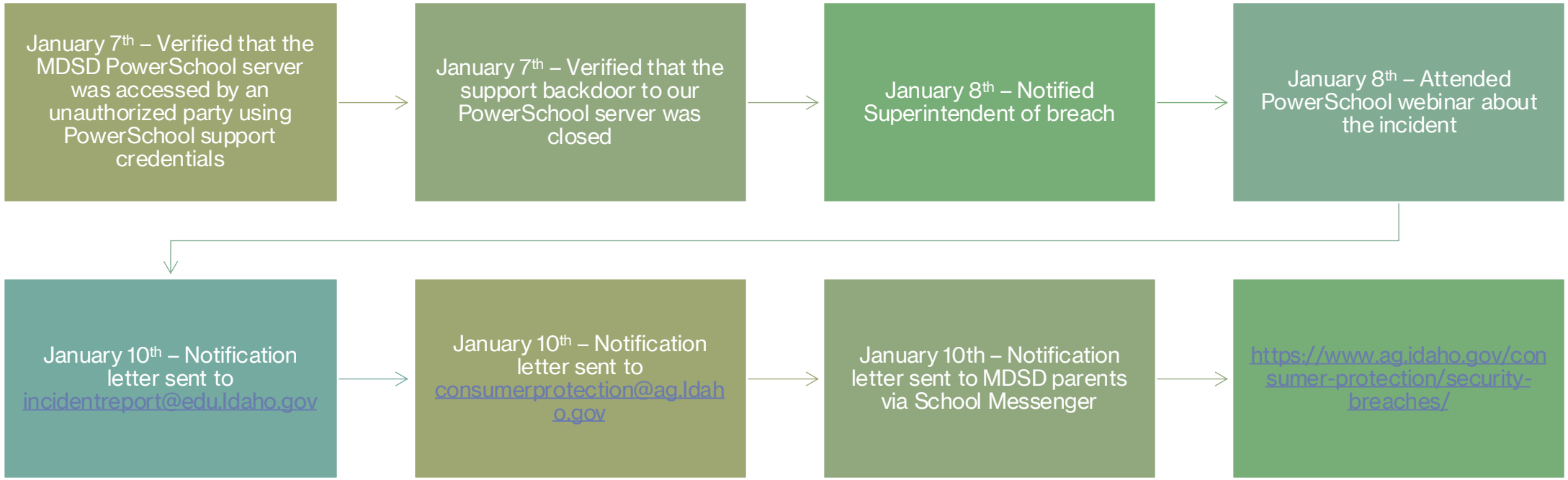
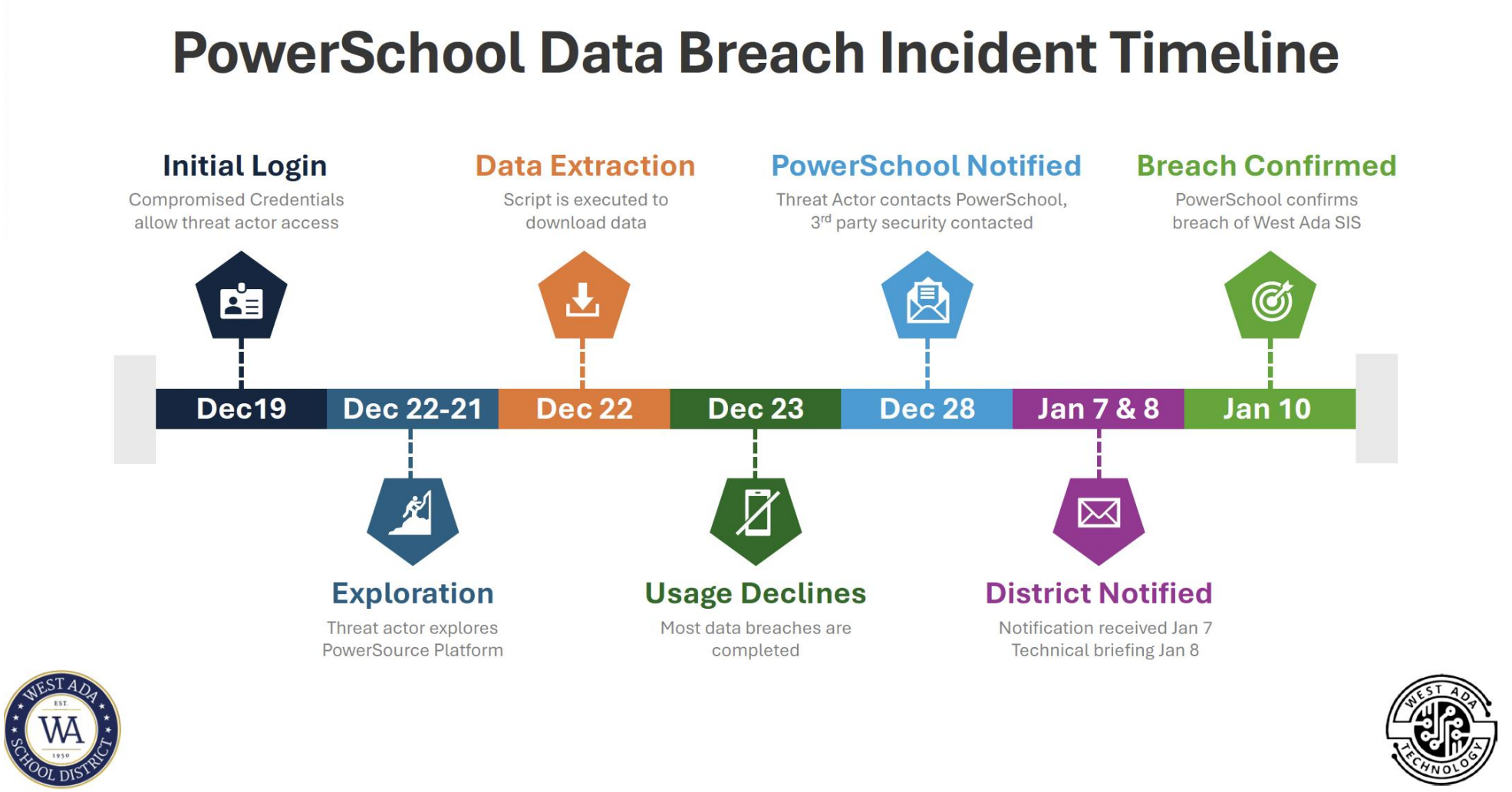
PowerSchool Breach

January 28, 2024

MDSD Timeline



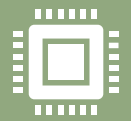
Borrowed from West Ada School District as their timeline matched ours



Breach Verification
Logs from MDSD PowerSchool Server

[Web Handler 508] 2024-12-22 19:57:36.32 UID=<<<NULL UID>>> IP=91.218.50.11 XFF=
URL=/public/home.html KV=ac:pearson-internal
P=powerschoolip|expires|serial|supportUser|caseNumber|signature|request_locale V=GET
EX=5823cddca6a3494a9ccc45036f8708dd

[Web Handler 496] 2024-12-22 19:57:52.49 UID=200A0 IP=91.218.50.11 XFF=
URL=/ws/md/v1/massdata/executeExport/Teachers_export.csv KV= P=request_locale V=POST
EX=9c18600cbcd541ca9191610efc548f93



Web Handler 508] 2024-12-22 02:34:34.587 UID=200A0 IP=91.218.50.11 XFF=
URL=/ws/md/v1/massdata/executeExport/Students_export.csv KV= P=request_locale V=POST
EX=afe8cfd97527431d9fd6adaffa0997be

Recommended Steps

Security Awareness Training for staff via KnowBe4. Time to complete is roughly an hour and is done online, like Safe Schools training

Update procedures for new employees to take security awareness training before signing into district systems

Roll out certificate-based authentication for PowerTeacher and PowerSchool Admin on district owned and managed devices. This allows staff to sign into PowerSchool with a certificate instead of a password, and does not require using a phone text code, authenticator app, or a USB security key

Recommend not allowing PowerTeacher and PowerSchool Admin unless it is from a district-owned device.

McCall-Donnelly SCHOOL DISTRICT

"Developing Lifelong Learners *Today*"

McCall-Donnelly Joint School District No. 421
299 S. 3rd St., McCall, ID 83638
Phone: (208) 634-2161 Fax: (208) 634-4075

Dear Office of the Attorney General:

I am writing to notify you that McCall-Donnelly School District 421 has experienced a data breach that resulted in some student and teacher personal information from our student information system (SIS) being compromised.

On Tuesday, January 7th, our IT department was notified by PowerSchool, our SIS provider, "that an unauthorized party gained access to certain PowerSchool Student Information System ("SIS") customer data using a compromised credential, and we regret to inform you that your data was accessed." Following this notification, our IT staff reviewed data access logs and found that this party had accessed data from two tables in our SIS, the Student table and the Teacher table.

On Wednesday, January 8th, we received a more in depth briefing from PowerSchool cyber security officials. In that briefing, they confirmed that only data from those two tables had been taken from affected school districts across the country and globe. They further stated that they had engaged the firms CyberSteward and CrowdStrike to investigate and respond to the cybersecurity attack. That response included engaging with the party who breached their system and negotiating an agreement through which the party destroyed the stolen data.

On the afternoon of January 8th, we notified current employees of the breach via email.

The backchannel connection to our PowerSchool SIS has been disabled. We are also reviewing other systems to ensure other such connections are not kept open. At this time, based on the information and recommendations provided to us by PowerSchool officials, we believe there is no ongoing threat related to this security breach.

Sincerely,

Timothy T Thomas
Interim Superintendent
McCall-Donnelly School District 421