Cybersecurity Priorities

Luke Wittum | Chief Information Officer, SET SEG

Mike Lilly | Associate Superintendent of Information Technology Services, Ingham ISD

Agenda

01 In the News

02 How Does a School Protect Itself From Threats?

03 Account Compromises

04 The Impact of AI With Cybersecurity

05 Industry Requirements and Reminders

Presenters

SET SEG & Ingham ISD

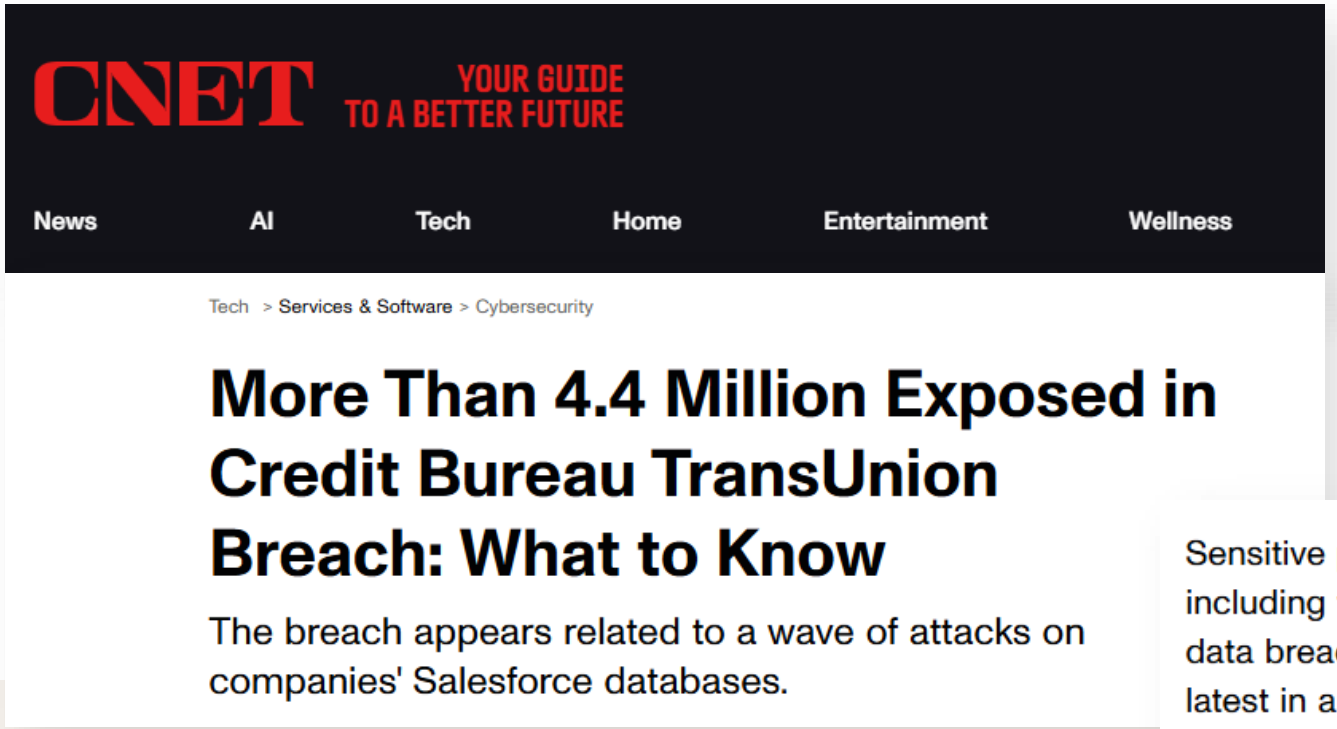
Luke Wittum
Chief Information Officer, SET SEG

lwittum@setseg.org
(517) 816-1608

Mike Lilly
Associate Superintendent of Information Technology Services, Ingham ISD

mlilly@inghamisd.org

In the News


CNET YOUR GUIDE TO A BETTER FUTURE

News AI Tech Home Entertainment Wellness

Tech > Services & Software > Cybersecurity

More Than 4.4 Million Exposed in Credit Bureau TransUnion Breach: What to Know

The breach appears related to a wave of attacks on companies' Salesforce databases.

"Breach caused by third party"

Sensitive personal information belonging to 4.4 million customers, including their names and Social Security numbers, was exposed in a data breach on credit bureau TransUnion, in what is believed to be the latest in a string of attacks targeting companies' Salesforce databases.

https://www.cnet.com/tech/services-and-software/more-than-4-4-million-exposed-in-credit-bureau-transunion-breach/

In the News

Forbes

16 Billion Apple, Facebook, Google And Other Passwords Leaked

By Davey Winder, Senior Contributor. Davey Winder is a veteran cybersecur... Follow Author

Published Jun 20, 2025, 07:07am EDT, Updated Jun 22, 2025, 06:22am EDT

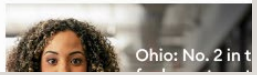
7 Add Us On Google

The biggest password leak in history confirmed.
GETTY

The 16 billion strong leak, housed in a number of supermassive datasets, includes billions of login credentials from social media, VPNs, developer portals and user accounts for all the major vendors, apparently. Remarkably, I am told that none of these datasets have been reported as leaked previously, this is all new data. Well, almost none: the 184 million password database I mentioned at the start of the article is the only exception. That has been contested by some cybersecurity professionals, but whatever the truth of the matter it remains a huge cause for concern

FORBES' FEATURED VIDEO

ADVERTISEMENT



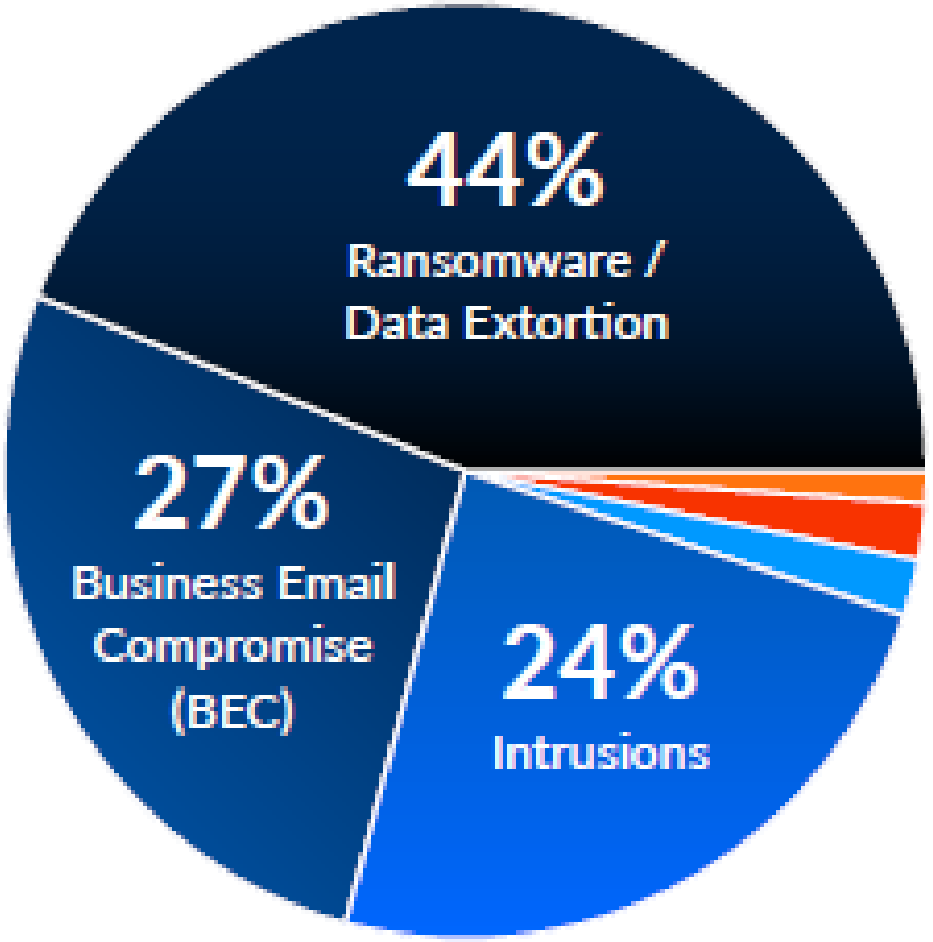
https://www.forbes.com/sites/daveywinder/2025/06/20/16-billion-apple-facebook-google-passwords-leaked---change-yours-now/

How Does a School Protect Itself From Threats?

Learning From Actual Cyber Incidents

Industry Insights

Note: “Intrusion” is classified as a ransomware attack that was detected and contained



Source: Arctic Wolf 2025 Threat Report

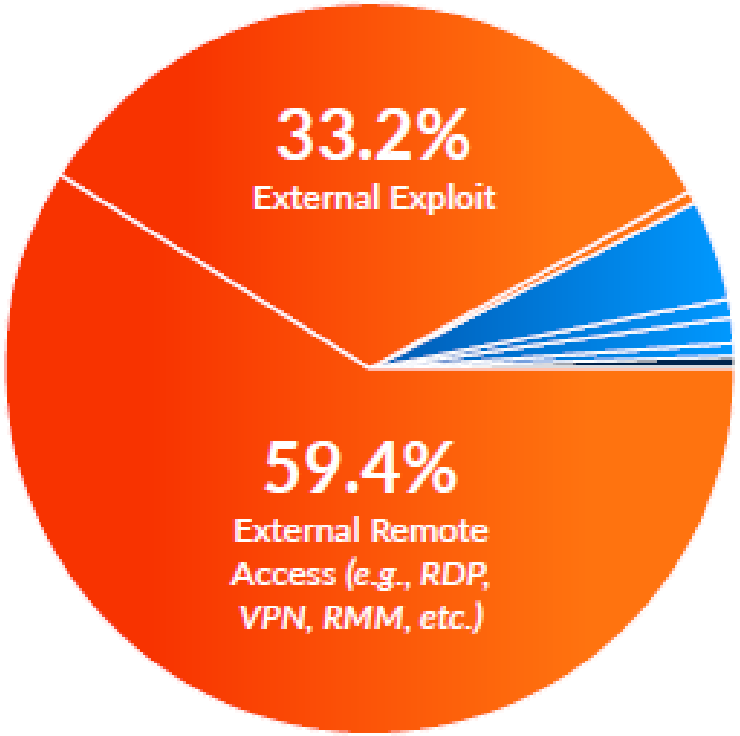
Actual Cybersecurity Incidents

Incident Description	Impact	Cost
Threat actor accessed district network through VPN without multi-factor authentication and used IT director credentials to deploy **ransomware**	District servers encrypted and data exfiltrated, ransom not paid	Over $100,000
Threat actor accessed district network through VPN without multi-factor authentication and deployed **ransomware**	Encrypted servers and exfiltrated 18GB of data, ransom not paid, 358 days open	Over $200,000
Threat actor accessed district network via remote desktop connection from a network shared server	Accessed credentials of 11 staff members with no data accessed or exfiltrated	Over $50,000
Threat actor accessed district network through shared VPN with the ISD	Movement through several servers with no data exfiltrated	Over $75,000
Threat actor accessed district network through vulnerable VPN software tied to HVAC controllers and deployed **ransomware**	Server encrypted with no data exfiltrated, ransom not paid	Over $25,000

How Could These Attacks Have Been Prevented?

Industry Insights

Root Causes of Ransomware & Data Extortion IR Cases



- 0.4% Zero-Day Exploit
- 4.4% Malicious Software Download
- 0.9% Previously Compromised Account / Credentials
- 0.9% Social Engineering *(e.g., Tech Support Scam, Account Creation, etc.)*
- 0.4% Phishing
- 0.4% Third Party and Supply Chain

CATEGORIES

93.0%
External Exposure

6.6%
Human Risk

0.4%
Trusted Relationship

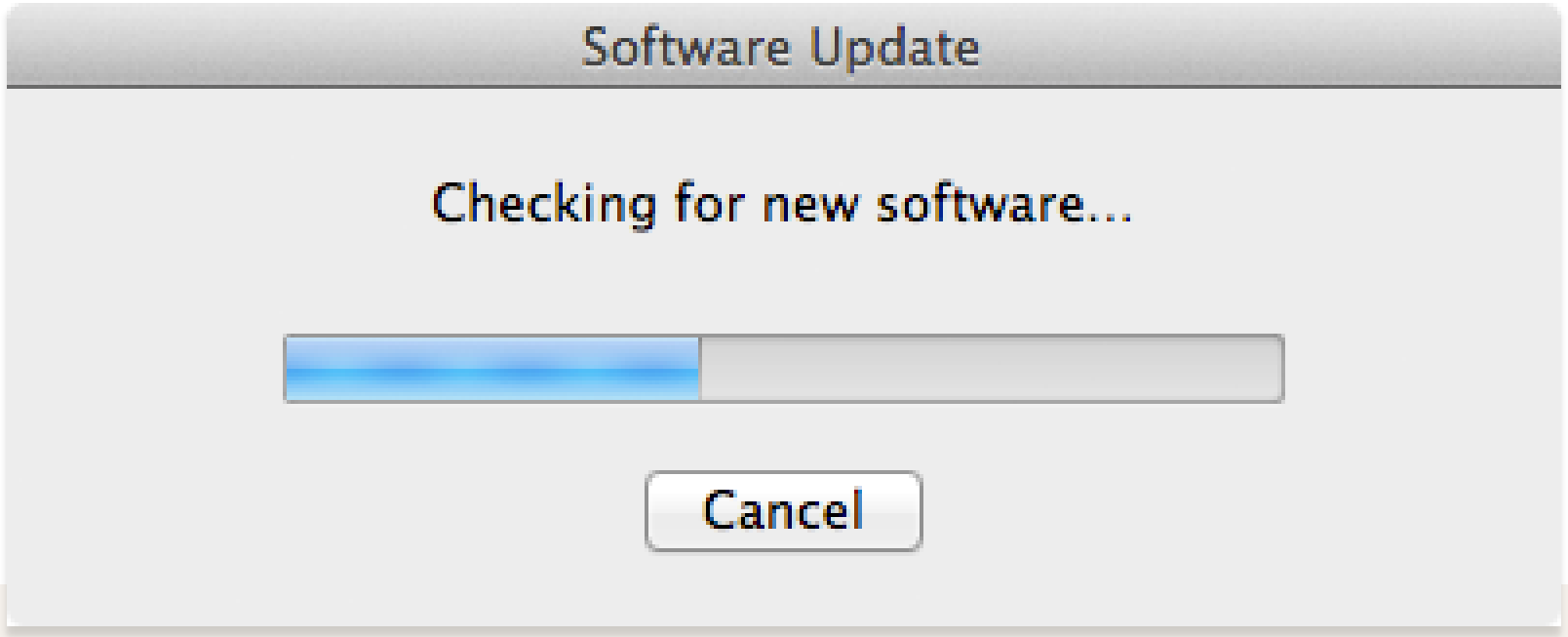
Source: Arctic Wolf 2025 Threat Report

Actual Cybersecurity Incidents

Incident Description	Impact	Cost
Vulnerability in new district monitoring software allowed threat actor to access network and deploy **ransomware**	Encrypted 120 workstations and 4 servers, school moved virtual for one week, ransom not paid, 508 days open	Over $240,000
Threat actor accessed district network through an open HS class web server port (undetected by vulnerability scan) and deployed **ransomware**	Servers encrypted, critical systems offline, school closed for 3 days, ransom not paid	Over $100,000
Threat actor accessed district network through HVAC server and moved through system before deploying **ransomware**	3 servers encrypted and data exfiltrated, ransom not paid, 582 days open	Over $150,000

How Could These Attacks Have Been Prevented?

Software Updates



Actual Cybersecurity Incidents

Incident Description	Impact	Cost
Vendor email was hacked and threat actor sent **fraudulent ACH payment instructions.**	District issued over $420,000 to criminal	Over $420,000
Threat actor accessed executive assistant's employee email account (may have been via their Disney+ account)	Data viewed and possible exfiltration, school closed for 1 day with no internet for additional 2 days	$30,000
Threat actor gained access to CFO's email account	CFO mailbox compromised with sensitive data viewed and possibly exfiltrated	$20,000
Email from threat actor posing as contractor with fraudulent ACH payment instructions.	District issued 2 payments totaling over $650,000 to criminal	Over $650,000

How Could These Attacks Have Been Prevented?

Financial Processes and Controls

SET SEG

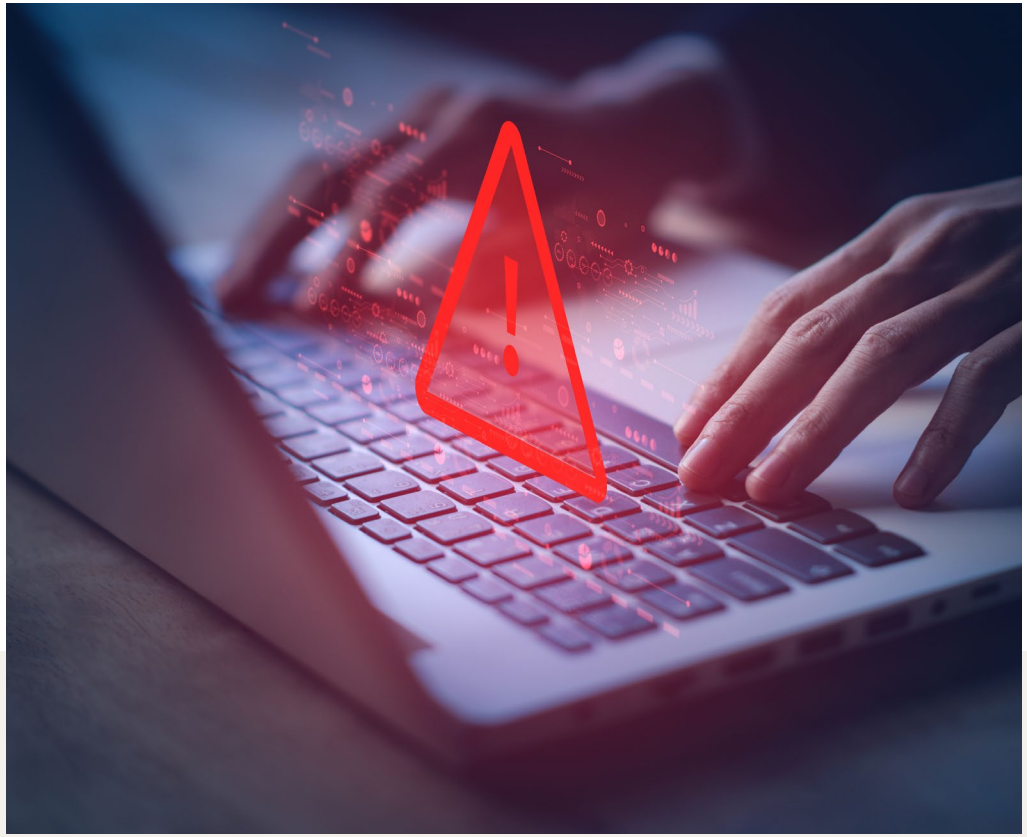
Account Compromise

Industry Insights

Root Causes of Business Email Compromise IR Cases

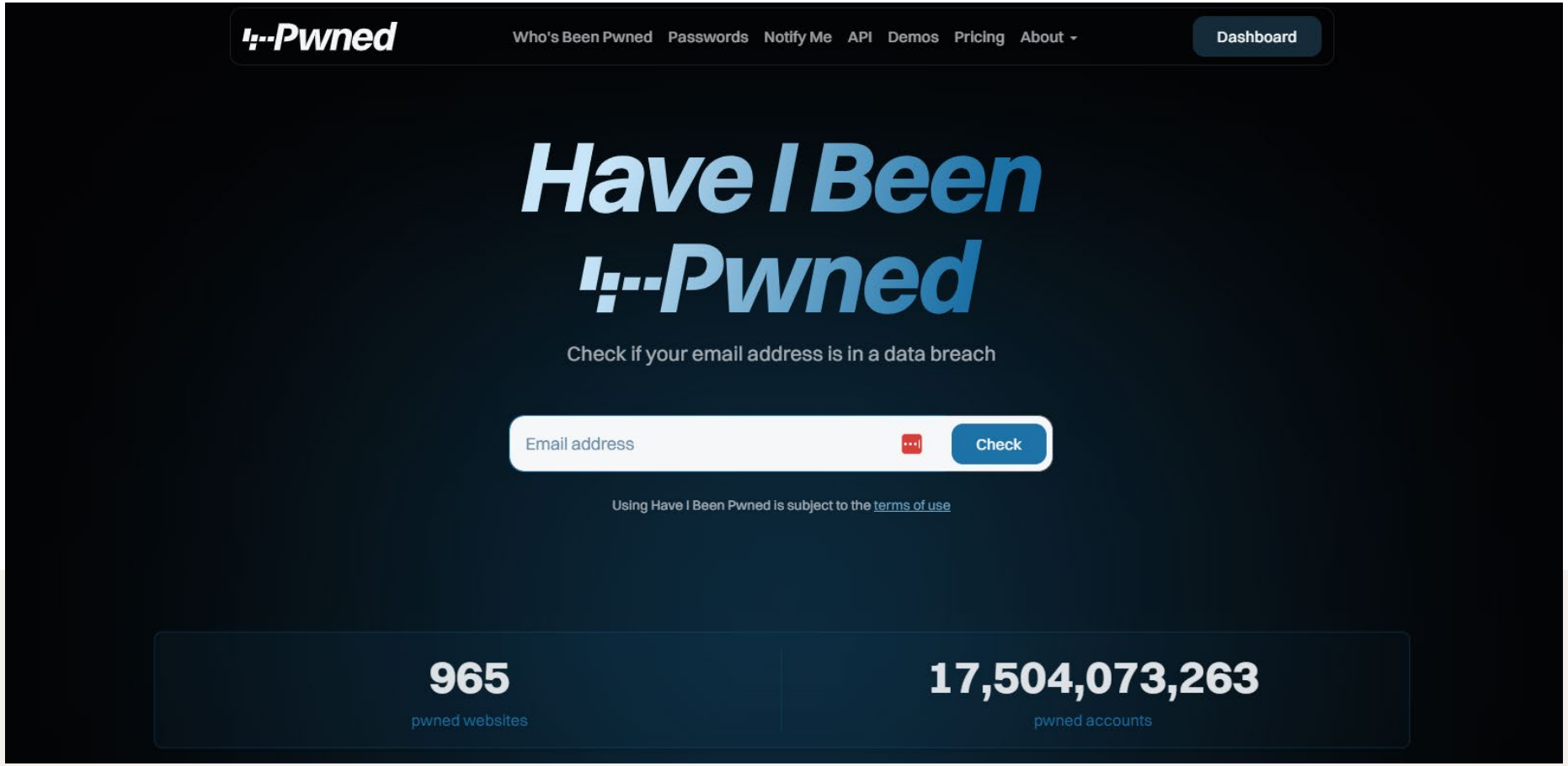
73.5%	Phishing
18.9%	Previously Compromised Account / Credentials
4.5%	Email Spoofing
2.3%	Social Engineering *(e.g., Tech Support Scam, Account Creation, etc.)*
0.8%	Malicious Insider

99.2% Human Risk **0.8%** Malicious Insider

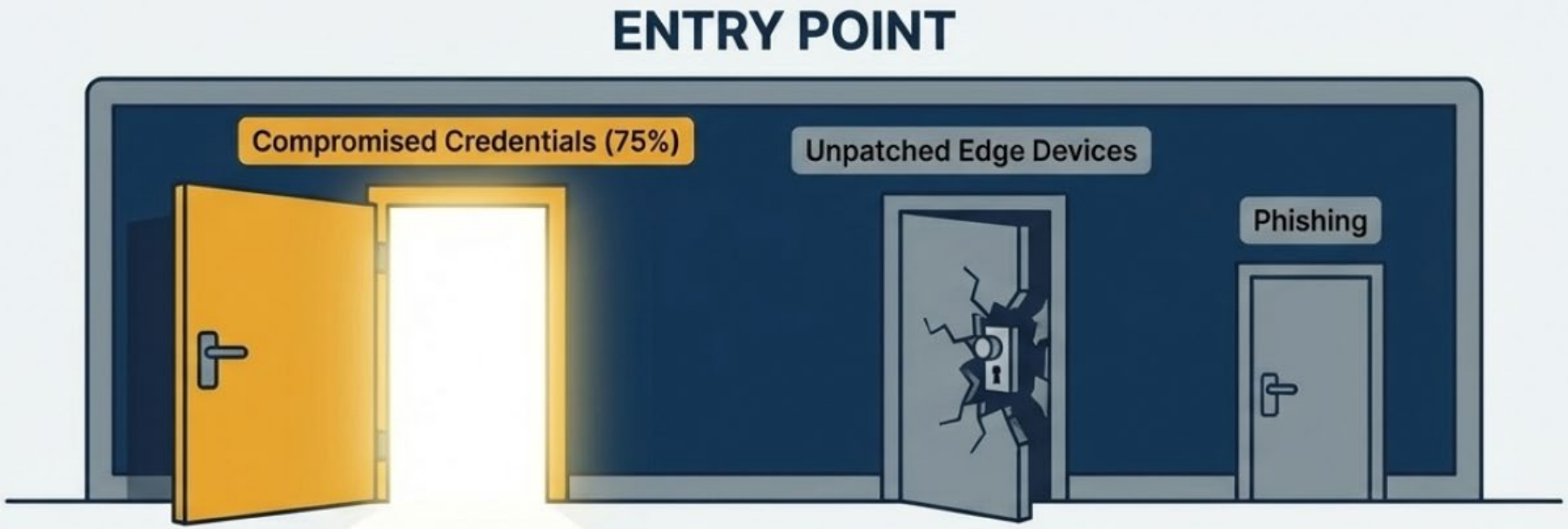


Source: Arctic Wolf 2025 Threat Report

https://haveibeenpwned.com/



Common Entry Points



Three-quarters of incidents originate from stolen passwords (MI SOC). Attackers harvest credentials when staff reuse their school passwords on personal sites that get breached.

The DBIR highlights a massive surge in exploiting vulnerable internet-facing systems, like outdated school VPNs originally set up for remote learning.

Protect Your District

2025 Michigan K12 Cybersecurity Incident Review

The MiSecure Security Operations Center (SOC) provides a team of cybersecurity analysts that manages and monitors the MDR platform. This includes district onboarding, responding to sensor alerts, and addressing high-severity vulnerabilities. In addition, the team is available to assist any Michigan K12 school district in their response to a cybersecurity investigation or confirmed incident. This report documents the findings based on 18 individual cybersecurity responses handled by the MiSecure SOC team.

Credentials

75% of the incidents originated with an account compromise. This pattern is consistent with other industries and other states. Users tend to still be the weakest area in our cyber defenses and the primary target for attackers. While we typically don't hear the details involved with the credential compromise. We suspect that an end-user has used their school email address and their school password on another site which was later compromised. Attackers "harvest" such credentials and use them to gain unauthorized access. Our recommendations include:

- Utilize the Identity module within Crowdstrike to monitor for compromised passwords
- Train users to use unique passwords
- Consider the use of password manager tools
- Require long, complex passwords
- Monitor for logins from unusual locations or devices
- Require occasional password changes - over half of the attacks would have been stopped by simply requiring MFA

- Multifactor Authentication
- Unique Passwords
- Complex Passwords
- Monitor Logins

Ransomware Guide

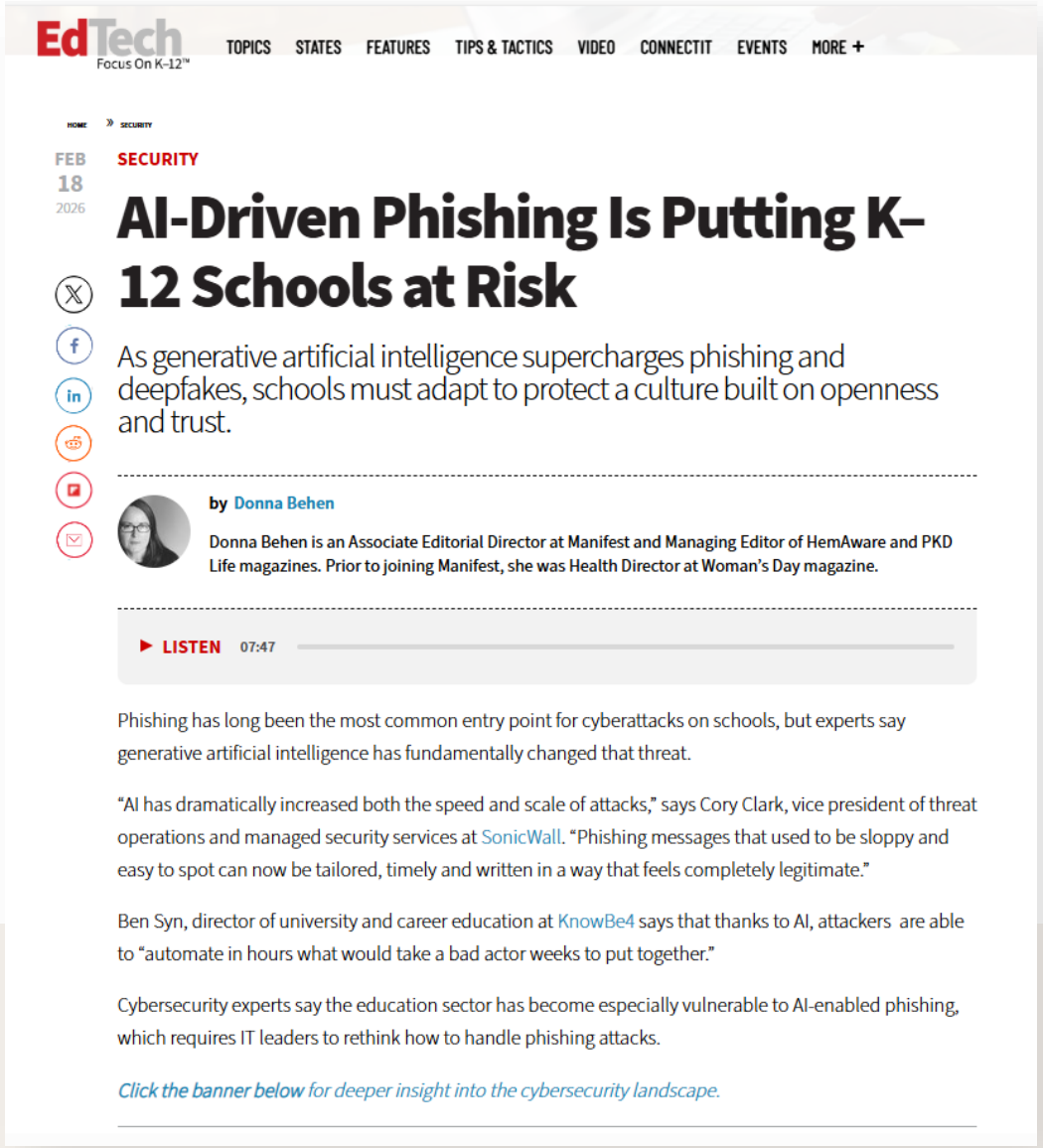
SET SEG

SET SEG

The Impact of AI With Cybersecurity

AI-Enhanced Phishing

"AI has removed red flags such as bad grammar or odd formatting."



EdTech Focus On K-12™ TOPICS STATES FEATURES TIPS & TACTICS VIDEO CONNECTIT EVENTS MORE +

HOME » SECURITY

FEB 18 2026

SECURITY

AI-Driven Phishing Is Putting K–12 Schools at Risk

As generative artificial intelligence supercharges phishing and deepfakes, schools must adapt to protect a culture built on openness and trust.

by Donna Behen

Donna Behen is an Associate Editorial Director at Manifest and Managing Editor of HemAware and PKD Life magazines. Prior to joining Manifest, she was Health Director at Woman's Day magazine.

▶ LISTEN 07:47

Phishing has long been the most common entry point for cyberattacks on schools, but experts say generative artificial intelligence has fundamentally changed that threat.

"AI has dramatically increased both the speed and scale of attacks," says Cory Clark, vice president of threat operations and managed security services at SonicWall. "Phishing messages that used to be sloppy and easy to spot can now be tailored, timely and written in a way that feels completely legitimate."

Ben Syn, director of university and career education at KnowBe4 says that thanks to AI, attackers are able to "automate in hours what would take a bad actor weeks to put together."

Cybersecurity experts say the education sector has become especially vulnerable to AI-enabled phishing, which requires IT leaders to rethink how to handle phishing attacks.

Click the banner below for deeper insight into the cybersecurity landscape.

SET SEG

Deep Fake Examples

What happened:

- High school students created a **fake video of a middle school principal delivering a racist rant.**
- The video spread on TikTok and triggered intense backlash from parents and the community.

Cybersecurity lesson:

- Students now have access to powerful generative AI tools.
- Deepfakes can create **false narratives about staff** that cause immediate community distrust.

Deep Fake Examples

What happened:

- A fake audio recording circulated online that sounded like the principal making racist and antisemitic remarks about students.
- The recording spread rapidly on social media and within the school community.
- Parents, students, and staff believed it was real before investigators determined it was AI generated.

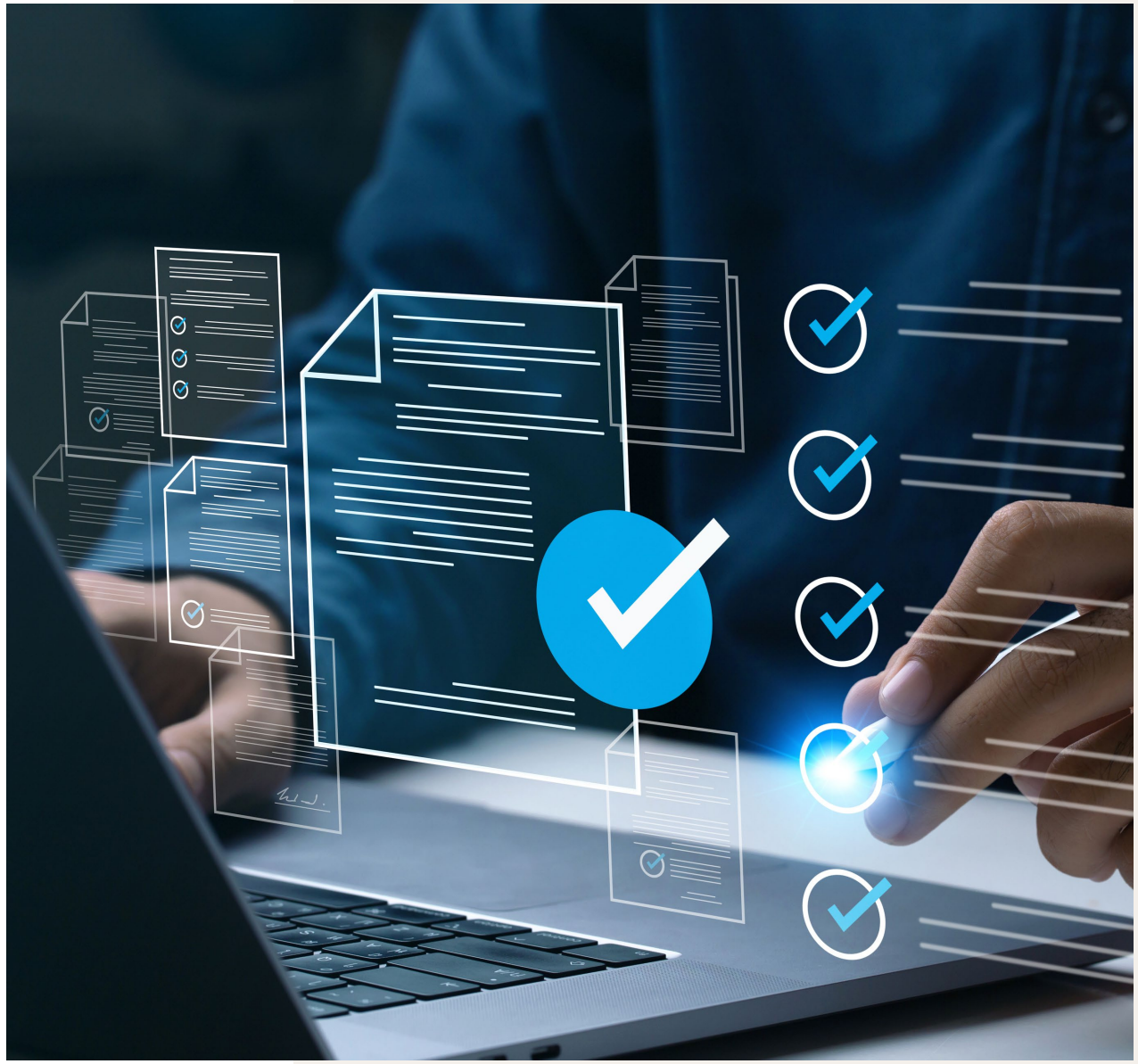
Outcome:

- The athletic director responsible was later sentenced to jail for creating the deepfake and disrupting school operations.

Cybersecurity lesson:

- Voice cloning can be used internally by disgruntled employees.
- Social media amplification can escalate the crisis within hours.
- Schools need crisis communication and digital forensics plans.

Reminders and Resources



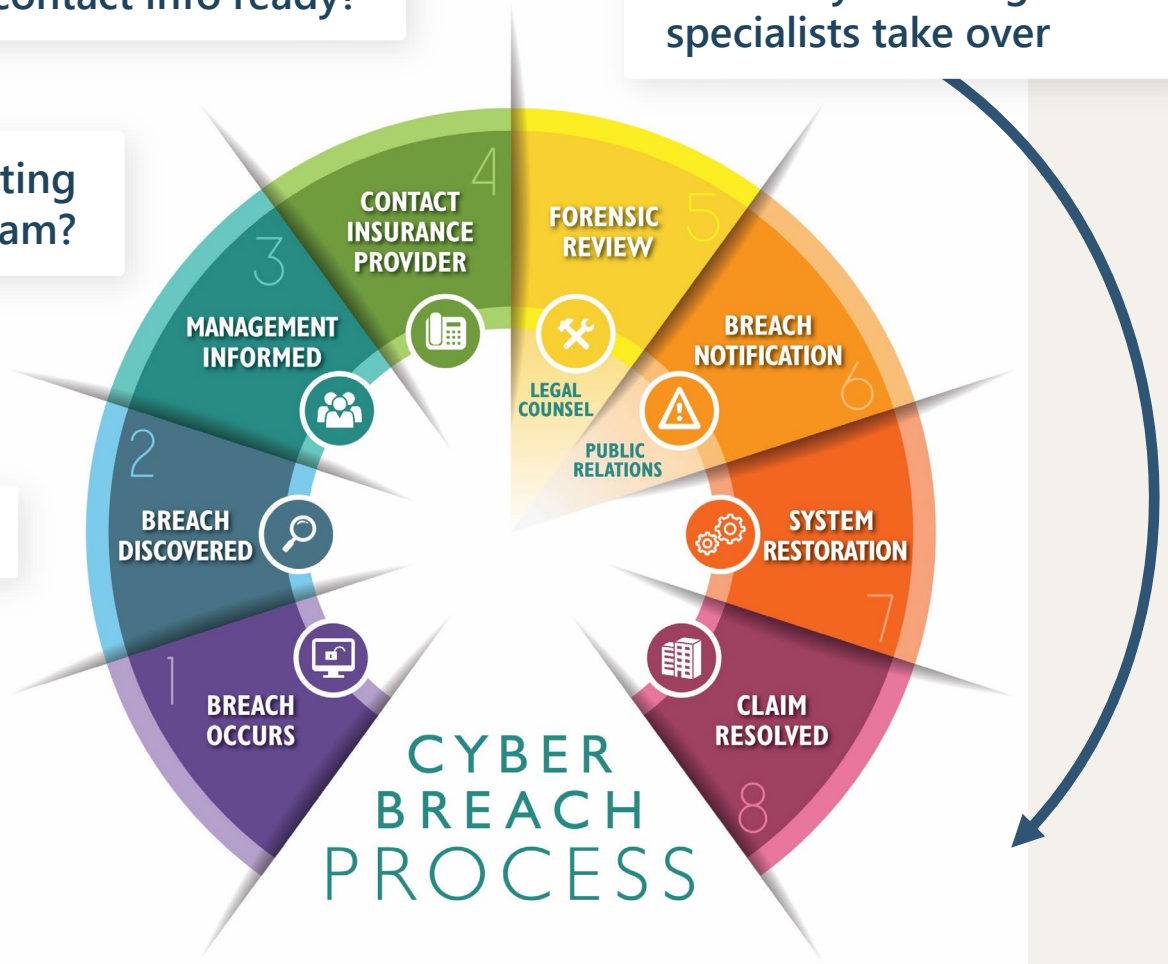
Cyber Breach Process

Do you have your insurer's contact info ready?

Let the cyber mitigation specialists take over

Who are you contacting within your team?

Incident Response Plan (IRP)



Resources for Schools by Schools

MiSecure
Managed Detection & Response
Incident Response Planning
Software Discounts – Abnormal, Lumu

MiCloud
Immutable Cloud Backups
AWS Cloud Server Hosting

MiSEN
Cyber Security Training Cohorts coming soon!

Industry Requirements & Reminders

- Phishing training
- Multifactor authentication (MFA) – remote access/critical information
- Backups offline/inaccessible to outsiders/encrypted/regularly scheduled
- Endpoint protection and response (EDR) and/or managed detection and response (MDR)
- Limiting administrative access
- System security patches updated
- Close open ports
- Vulnerability scans …

Pillar 1: Protect the Identities

- Because **75%** of attacks utilize stolen credentials, Multifactor Authentication (MFA) is the single most critical defense mechanism.
- **Over half** of all K-12 credential attacks would have been stopped simply by requiring MFA.
- **The baseline requirement:** Require MFA for all remote network access (VPNs), external-facing applications, and every administrator account. Phishing-resistant MFA is the ultimate goal.

Pillar 2: Safeguard the Network and Build Resilience

From Prevention to Rapid Recovery

- If the attacker breaches the perimeter, the district should be equipped to limit the operational damage and recover quickly.

Pillar 3: Incident Response and Human Defense

Know the Plan. Practice the Response.

Do not wait until the network in encrypted to figure out who is in charge.

- **The written plan:** Every district should have a written **incident response plan (IRP)** that outlines roles, responsibilities, and communication strategies (including how to contact your insurer and legal counsel).
- **Practice makes perfect:** Conduct regular tabletop exercises with district leadership to rehearse the plan.
- **Human firewall:** Implement continuous training campaigns to help staff recognize phishing attempts and handle data securely.

Questions?

Thank You

Contact

lwittum@setseg.org
(517) 816-1608

mlilly@inghamisd.org

Address

1520 Earl Ave.
East Lansing, MI 48823