OSSEO AREA SCHOOLS
ISD 279

Agenda Independent School District 279 School Board	Regular Business Meeting Educational Service Center - Forum Room 11200 93rd Ave N Maple Grove, MN 55369 Tuesday, October 8, 2024 6:00 PM

Our mission is to inspire and prepare each and every scholar with the confidence, courage and competence to achieve their dreams; contribute to community; and engage in a lifetime of learning.

This regular meeting of the Osseo School Board is being conducted the Board Room of the Educational Service Center, and is open to the public. The meeting can be monitored electronically by streaming online at district279.org/info-center/school-board (Watch Livestream). An archived recording will also be available on the district website.

Agenda Items

1. 6:00 p.m. Welcome and purpose
   Tanya Prince, Board Vice Chair
2. 6:05 p.m. Check in
   Dr. Kim Hiel, Superintendent
3. 6:05-6:45 p.m. English Language Arts (ELA) Curriculum and Structured Literacy Review 2
   Dr. Bryan Bass, Assistant Superintendent of Equity and Achievement and Dr. Jill Kind, Director of Learning and Achievement
4. 6:45-7:30 p.m. Cyber Security 16
   Anthony Padrnos, Executive Director of Technology and Gerald Edwards, Director of Information Systems and Security
5. 7:30 p.m. Board meeting calendar review 134
   Dr. Kim Hiel, Superintendent
6. Adjournment
   Tanya Prince, Board Vice Chair

To accommodate individuals with disabilities, this material will be made available in alternative formats upon request. Individuals with disabilities are invited to request reasonable accommodations to participate in or attend a district activity, call your local school or the school district at least seventy-two (72) hours in advance (two-week notice preferred). Members of the public can view and download School Board meeting notices and regular meeting agendas and materials from the district website www.district279.org, under "Info Center > School Board."

ISD 279

OSSEO AREA SCHOOLS

ISD 279

Elementary Reading Curriculum

Learning & Achievement

School Board Work Session, October 8, 2024

Outcome of Presentation

- Board members will:
  - learn more about the structured literacy approach to reading instruction
  - gain an overview of our new elementary curriculums 95 Phonics Core and CKLA

Structured Literacy

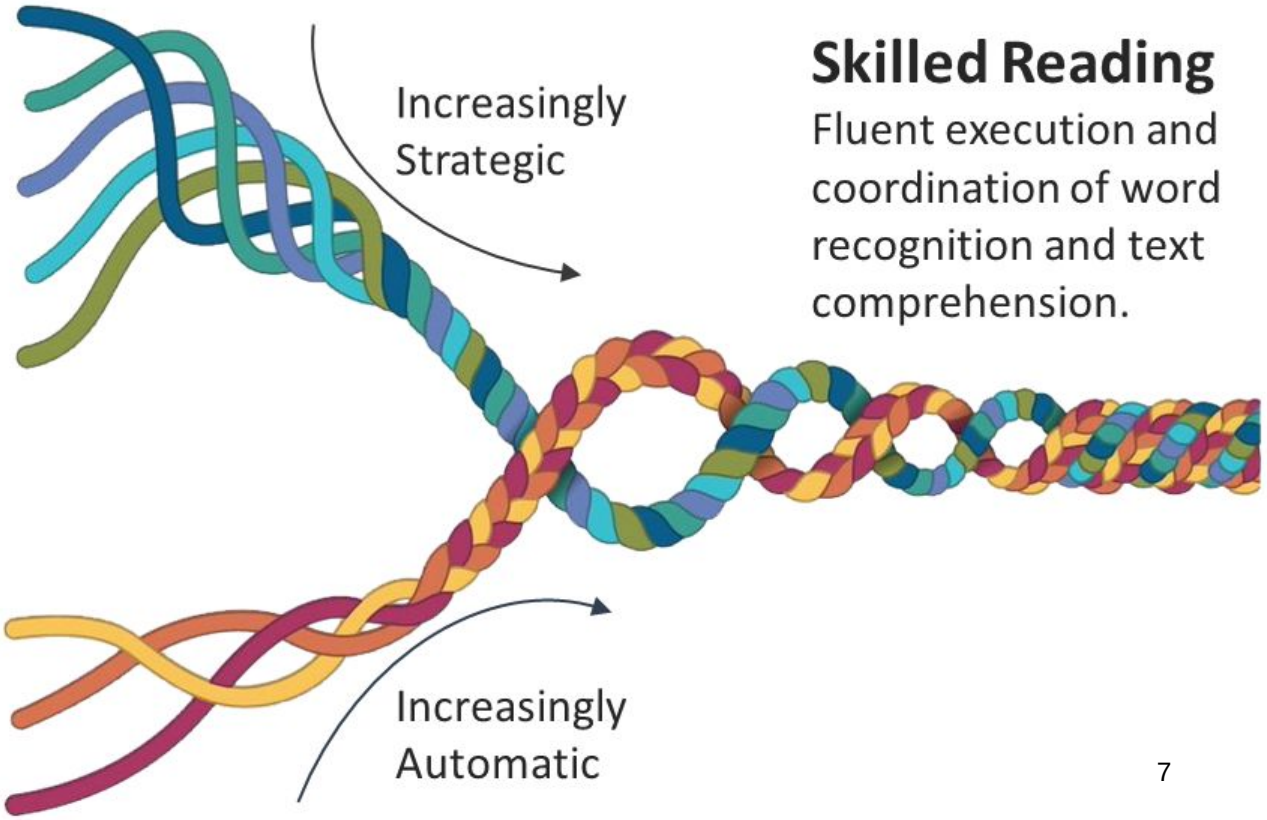
Structured Literacy

- Grounded in the Science of Reading research

SIMPLE VIEW OF READING

Language Comprehension

- Background Knowledge
- Vocabulary Knowledge
- Language Structures
- Verbal Reasoning
- Literacy Knowledge



Skilled Reading

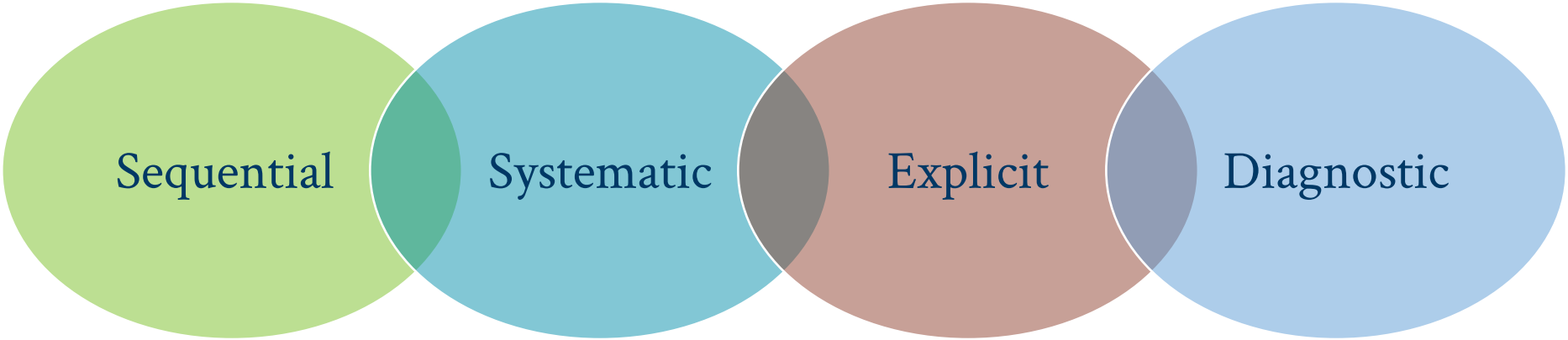
Fluent execution and coordination of word recognition and text comprehension.

Word Recognition

- Phonological Awareness
- Decoding (and Spelling)
- Sight Recognition

Scarborough, H. 2001. Connecting early language and literacy to later reading (dis)abilities: Evidence, theory, and practice. Pp. 97-110 in S. B. Neuman & D. K. Dickinson (Eds.) *Handbook of Early Literacy.* NY: Guilford Press.

Structured Literacy



Structured Literacy

- Grounded in the Science of Reading research
- MN READ Act
  - Curricular Resources
  - Interventions
  - Screenings
  - Professional Learning
  - Family and Community Engagement
  - Local Literacy Plan
  - Dyslexia

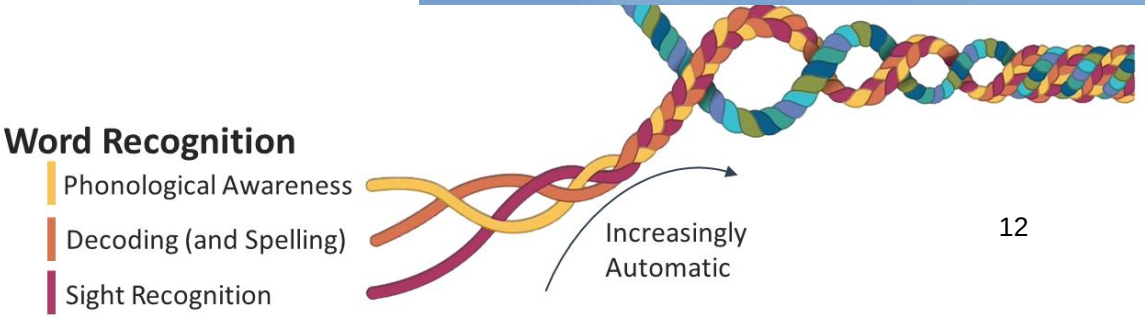
95 Phonics Core & CKLA

Process

- Began in 2021-2022 school year, learning about structured literacy and resources
- Failed pilot in 2022-2023
- Successful pilot in 2023-2024
- Professional learning for all teachers

95 Phonics Core

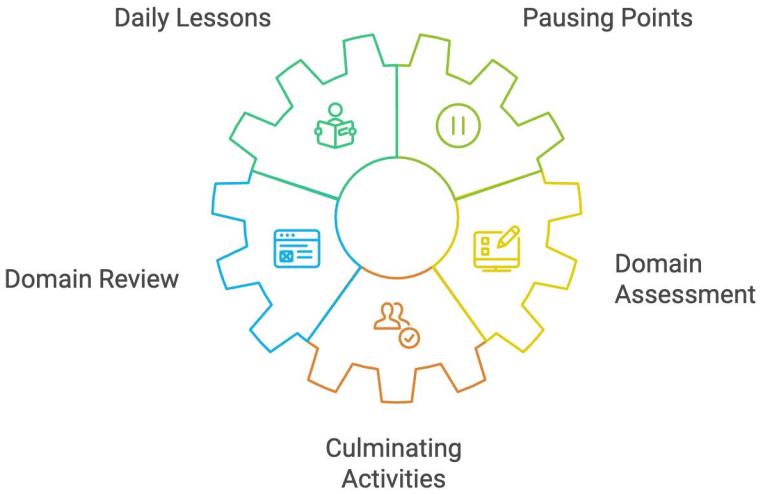
- Word Recognition strand – (Foundational)
- 30 minutes daily
- Phonics

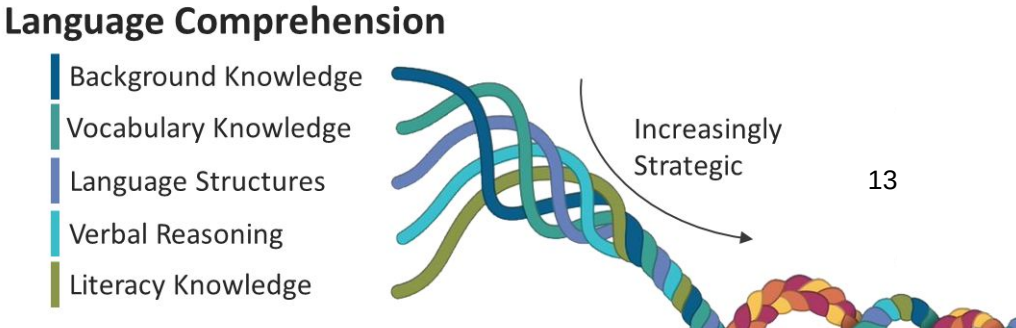


Scarborough, H. 2001. Connecting early language and literacy to later reading (dis)abilities: Evidence, theory, and practice. Pp. 97-110 in S. B. Neuman & D. K. Dickinson (Eds.) *Handbook of Early Literacy.* NY: Guilford Press.

CKLA

- Language Comprehension
- Embedded supports for students in multilingual programs and special education





Literacy Block

Literacy Block (ELA Grade Level Standards)	120 Literacy Minutes	
95 Phonics Core (Word Recognition Skills)	30 minutes per day	Gradual Release Model (I Do/We Do/You Do)
Amplify CKLA (Knowledge and Language Comprehension)	60 minutes per day	
Differentiated Instruction/Independent Work Time	30 minutes per day	

ISD 279

OSSEO AREA SCHOOLS

ISD 279

Questions or Comments?

TO: Osseo Area Schools Board
FROM: Anthony Padrnos; Executive Director of Technology
Gerald Edwards; Director of Information Systems & Security
SUBJECT: Cybersecurity Update
DATE: October 8, 2024

The 2024 cybersecurity update provides an overview of the current K-12 cybersecurity landscape, the state of cybersecurity in Osseo Area Schools, and the district's ongoing efforts to protect digital assets. The key objectives are to inform the Board of recent trends, current challenges, and ongoing initiatives to enhance cybersecurity posture within the district.

K-12 Cybersecurity Landscape: Educational institutions face growing cybersecurity threats, with ransomware and malware being top attack vectors. Nationally, there have been over 1,600 reported incidents in K-12 schools since 2016, with recent incidents impacting school districts in Minnesota, including Elk River, Rochester, and Minneapolis.

Current State of Cybersecurity in Osseo Area Schools: Osseo Area Schools has established a comprehensive cybersecurity framework through strategic partnerships with industry leaders such as Red Canary, MS-ISAC, and participation in the West Metro Security Consortium. Key tools and services include continuous monitoring, threat detection, and proactive incident response.

Cybersecurity Initiatives:

1. **Training**: Annual digital security training is provided to all employees. Additionally, tabletop exercises have been introduced for district and school leadership to enhance preparedness.
2. **Monitoring**: Regular assessments are conducted, including monthly external scans, quarterly phishing tests, and the deployment of Microsoft and Red Canary Endpoint Detection and Response (EDR/MDR) solutions.
3. **Response**: A comprehensive digital security plan is in place, including an incident response plan, routine backup recovery testing, and continuity plans at both the district and site levels.

These initiatives reflect our ongoing commitment to ensuring digital security across all aspects of the educational environment, safeguarding student and staff data, and minimizing disruption due to cyber incidents.

Att.

- Board Update Slides
- 2022-23 K-12 Report from MS-ISAC and CIS
- 2022 State of K12 Cybersecurity from K12 Six
- 2023 Internet Crime Report from FBI

ISD 279

OSSEO AREA SCHOOLS

ISD 279

Cybersecurity Update

October 8, 2024

Objectives

- Board will learn about the current K-12 Cybersecurity landscape
- Board will be informed on the current state of Cybersecurity in Osseo Area Schools
- Board will be aware of current Cybersecurity work in Osseo Area Schools

K-12 Cybersecurity Landscape

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

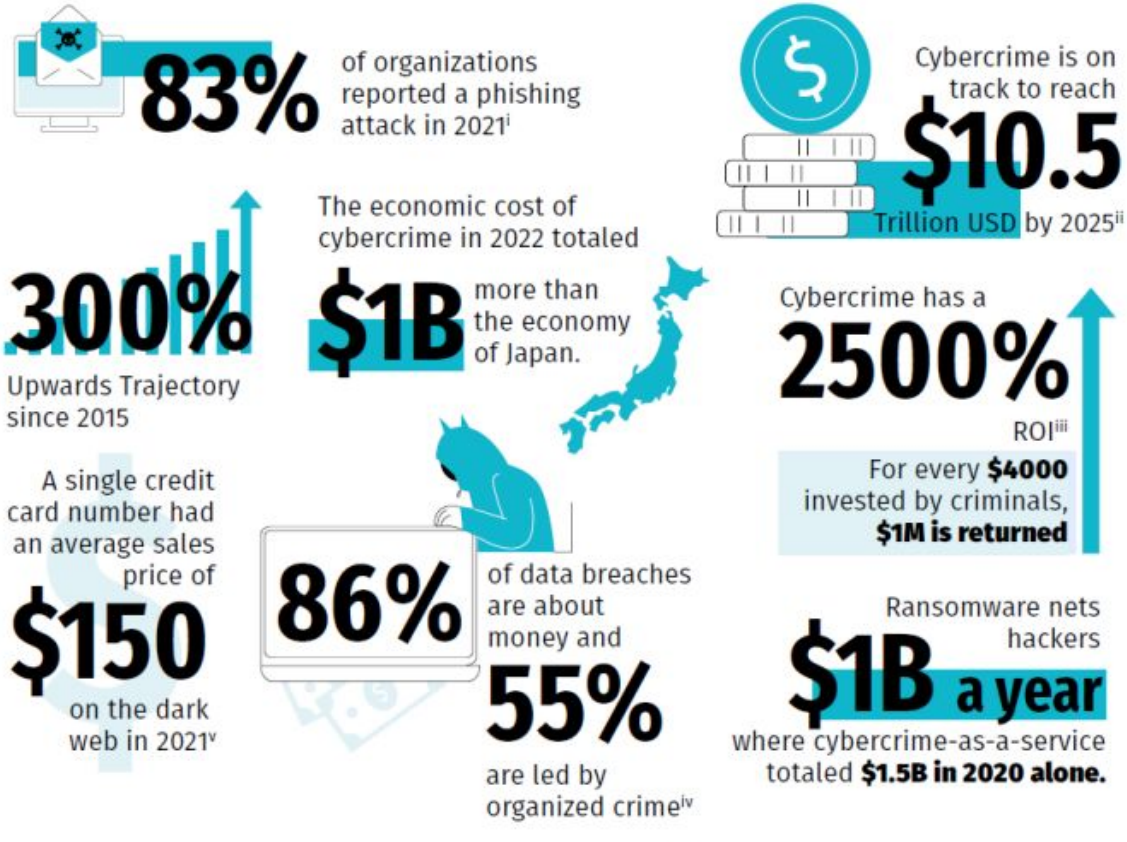
Critical Infrastructure Sectors

1. Chemical
2. Commercial Facilities
3. Communications
4. Critical Manufacturing
5. Dams
6. Defense Industrial Base
7. Emergency Services
8. Energy
9. Financial Services
10. Food and Agriculture
11. Healthcare and Public Health
12. Information Technology
13. Nuclear Reactors, Materials, and Waste
14. Transportation Systems
15. Water and Wastewater
16. Government Facilities & K12

The ROI of Cybercrime

Where there is profit, there is opportunity.

The economic impact of cybercrime has tripled in the past decade. No longer the hacker in a hoodie, today's threat actor is a professional. Structured and top line focused, organized cybercriminals act as an enterprise – following the same rules of finance as their targets.



Infographic source: The ROI of Cybercrime (www.sans.org)

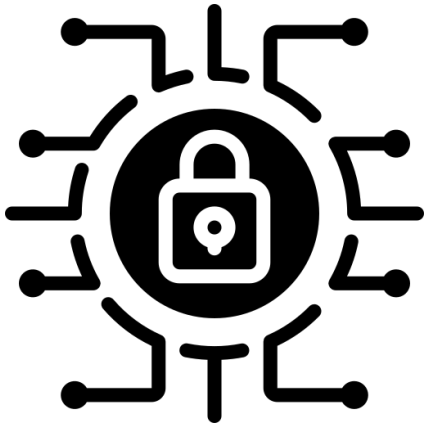
Top Five K-12 Security Concerns

K-12 respondents to the 2022 NCSR reported their top five security concerns as follows:

Lack of sufficient funding	81% of participants
Increasing sophistication of threats	59% of participants
Lack of documented processes	58% of participants
Lack of a cybersecurity strategy	47% of participants
Inadequate availability of cybersecurity professionals	41% of participants

Data timeframe: July 1, 2022 – June 30, 2023

CoSN 2024 Leadership Report

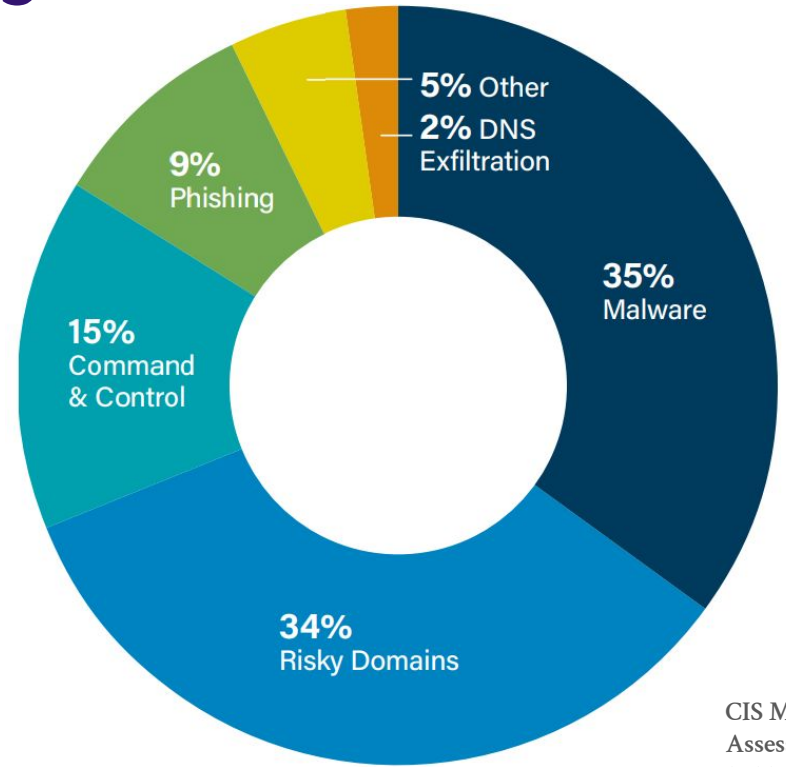


#1
Cybersecurity

#2
Data Privacy & Security

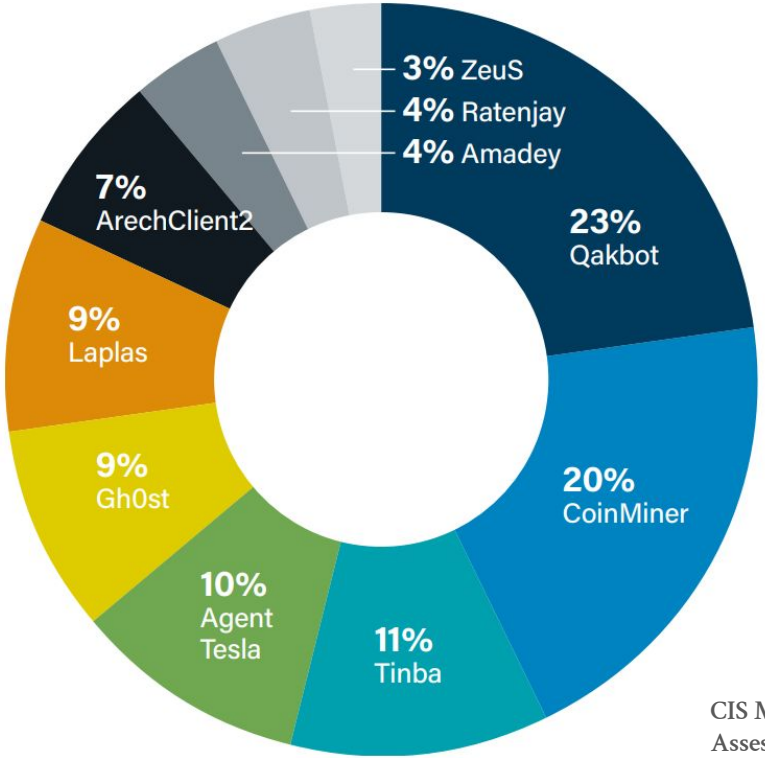
#5
IT Crisis Preparedness

Security Attack Trends in K-12



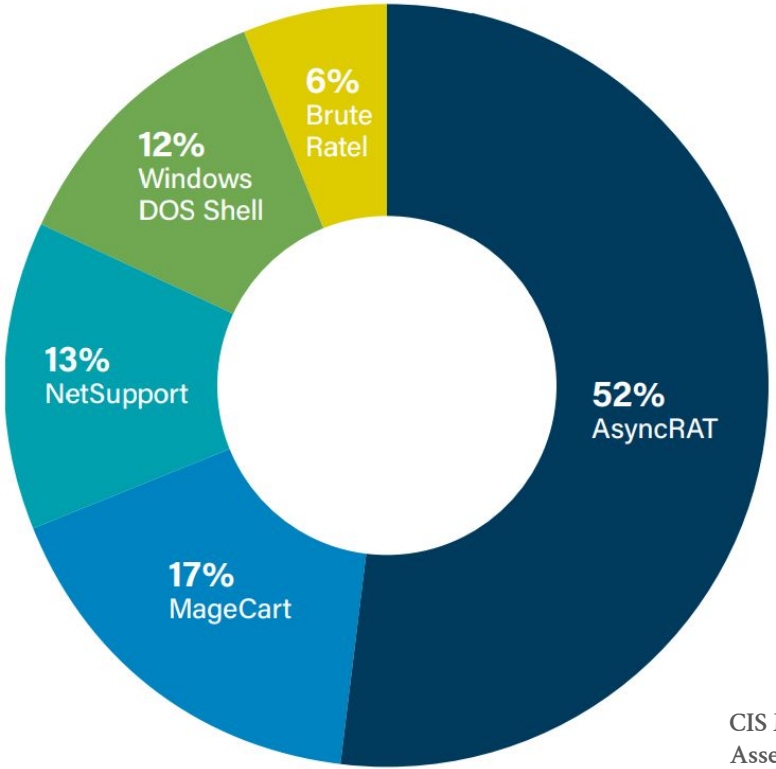
CIS MS-ISAC Cybersecurity Assessment of the 2022–2023 School Year

Top 10 Malware Attacks in K-12



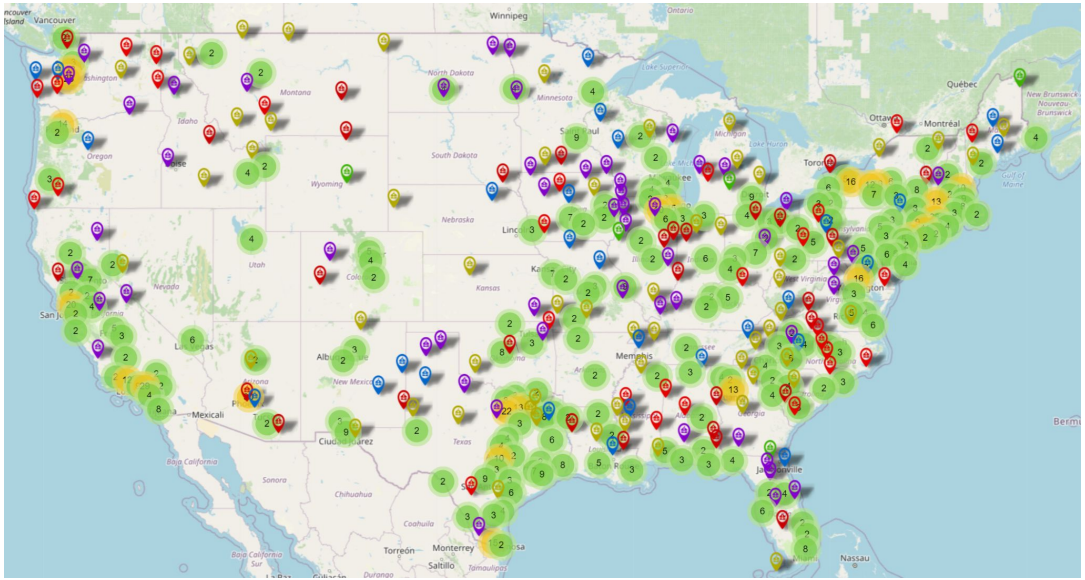
CIS MS-ISAC Cybersecurity Assessment of the 2022–2023 School Year

Top 5 Other Attacks in K-12



CIS MS-ISAC Cybersecurity Assessment of the 2022–2023 School Year

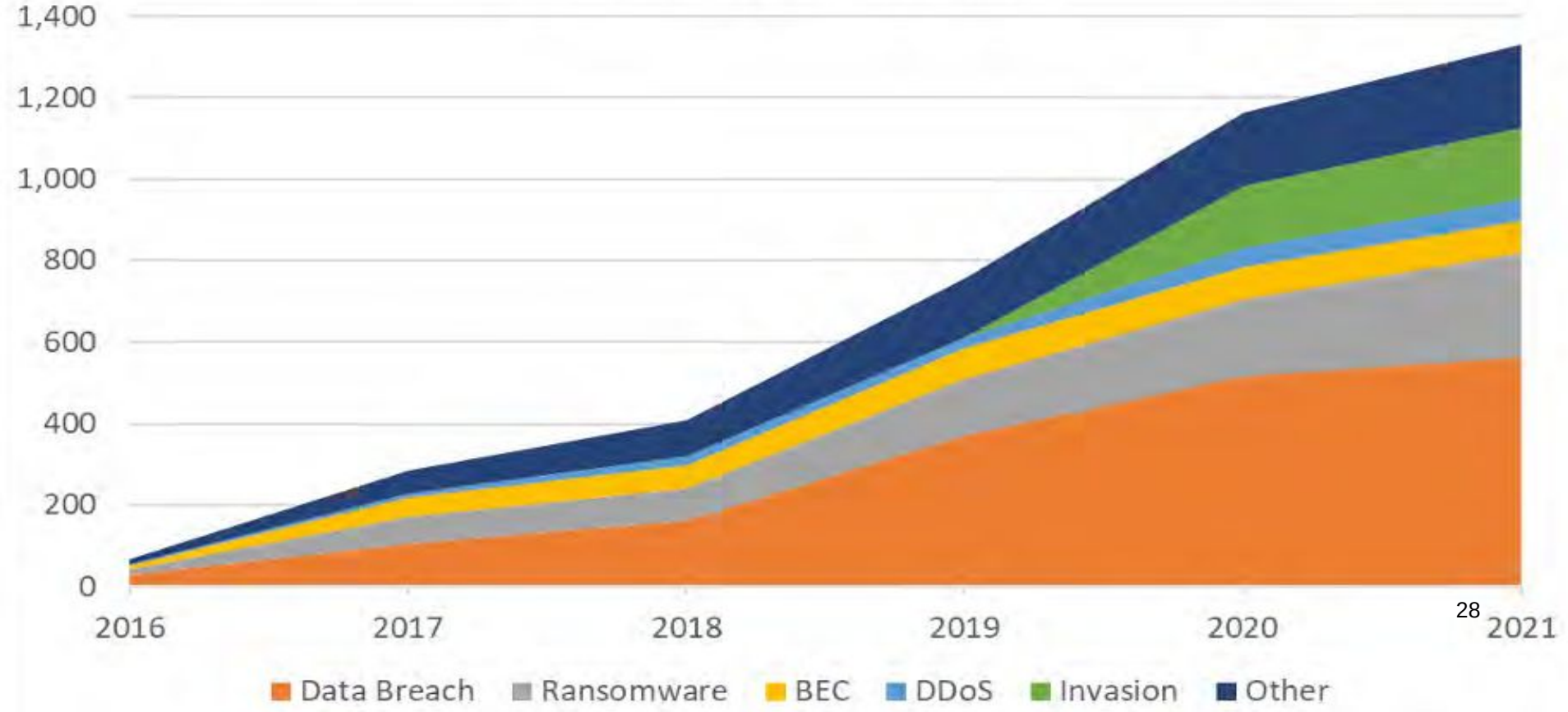
K-12 Publicly Reported Incidents



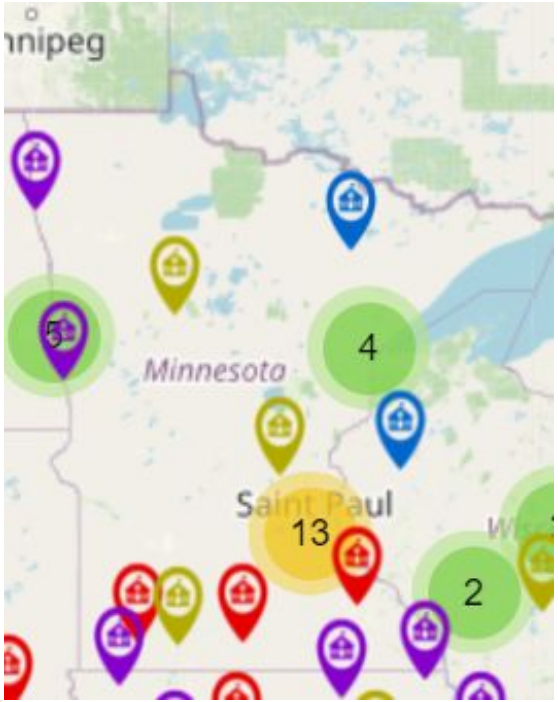
- 1,619 public incidents in K-12 schools since January 2016
- 32 in Minnesota

Source: K-12 Cybersecurity Resource Center

Number of Publicly-Disclosed K-12 Cyber Incidents by Incident Type: 2016-2021

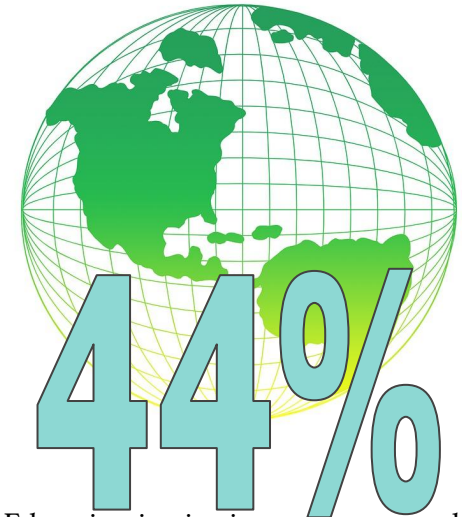


Recent K-12 Cyber Incidents in MN



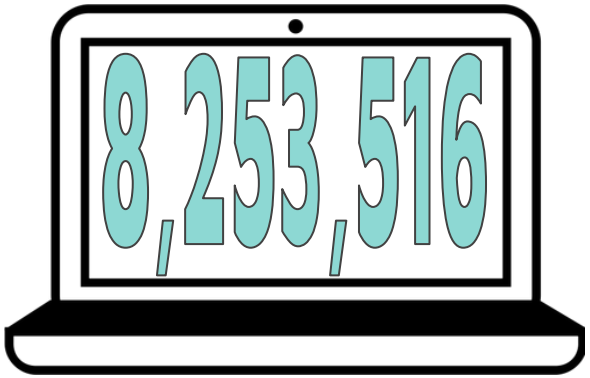
- Elk River
- Minneapolis
- Rochester
- Cloquet
- ARCC

The State of K-12 Cybersecurity



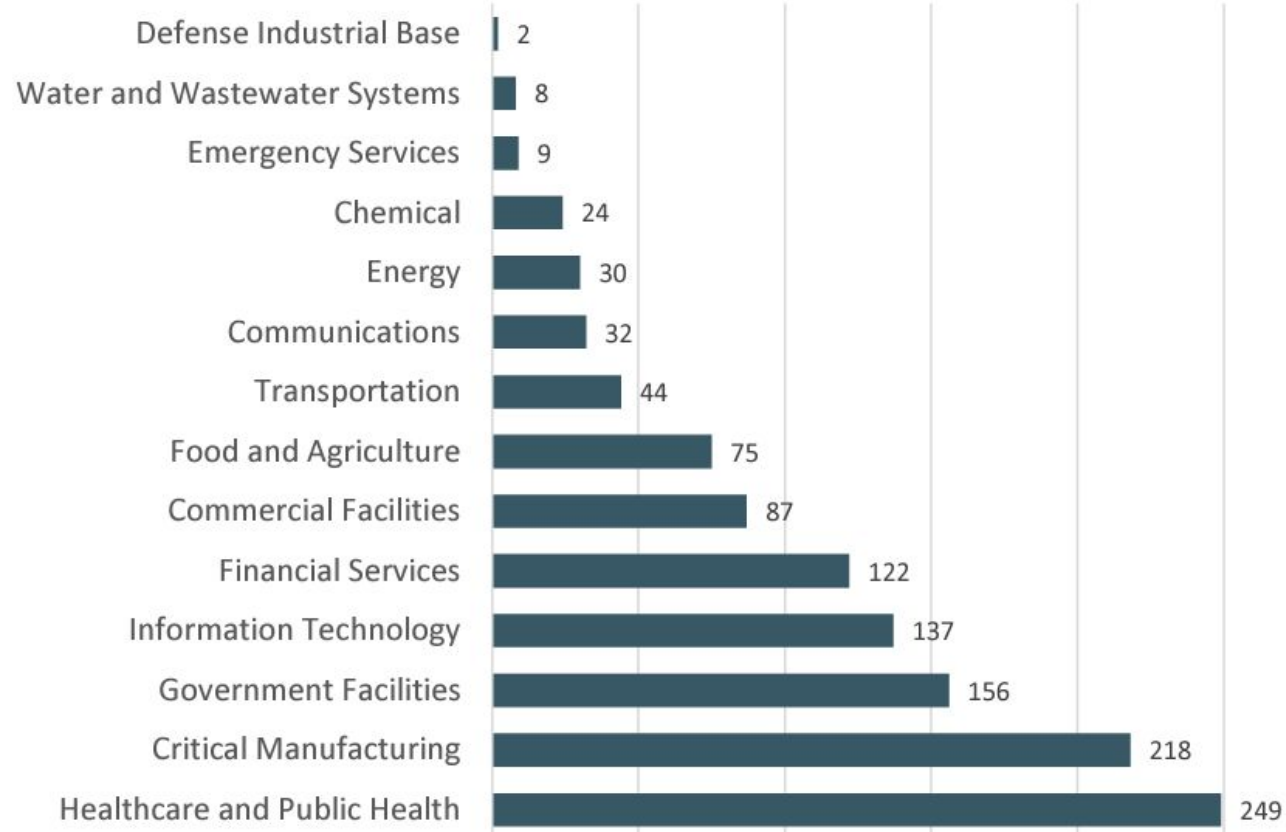
Education institutions were targeted by ransomware attacks in 2020 (Sophos)

Cost of downtime, repairs, and lost opportunities in 2020 ransomware attack in education (Sophos)



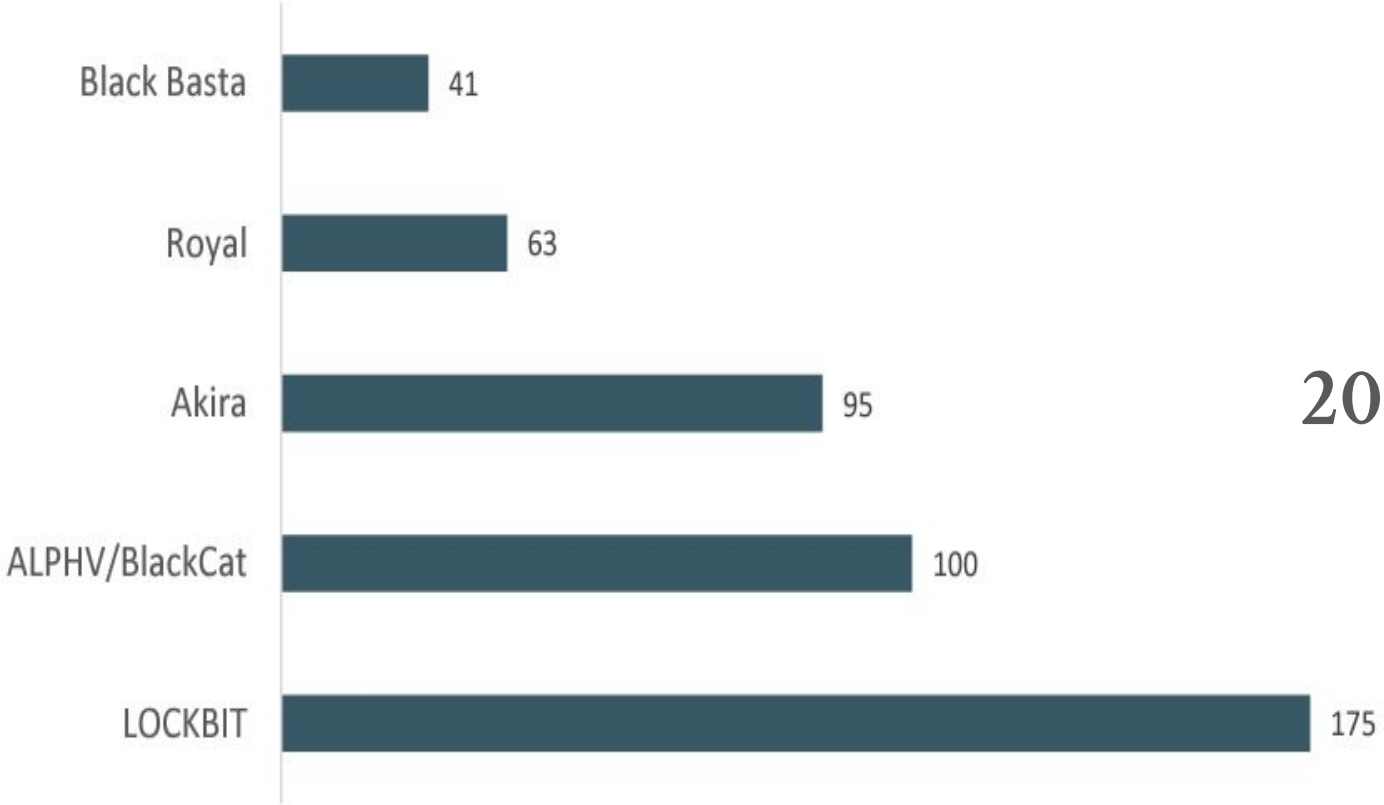
Number of devices in education that experienced malware over 30 days in December of 2021 (Microsoft Security Intelligence)

Sectors Affected by Ransomware



2023 FBI Report

Top Ransomware Attackers



2023 FBI Report

State of Cybersecurity in Osseo Area Schools

Cybersecurity Partners

Red Canary

Dark Knight

CISA

MS-ISAC

West Metro Security Consortium

Key Security Tools

Background: Endpoint Collection

Custom range July 1, 2023 - June 30, 2024

13 billion+
telemetry records

Raw Telemetry

Endpoint Footprint

Microsoft Defender for Endpoint, Microsoft Office 365, and Google Workspace sensors are deployed on 5,278 endpoints.

Monitored endpoints include:
- 100% Windows
- <1% Unknown

Key Takeaways

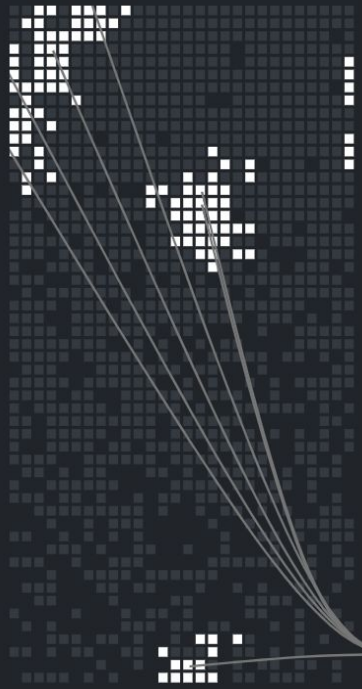
We processed 27 TB of telemetry from your endpoints, consisting of 13 billion+ telemetry records.

Processing this amount of data using a cloud SIEM would cost roughly $142,500 / year.

Background: Intelligence & Detection Engineering

Custom range July 1, 2023 - June 30, 2024

13 billion+
telemetry records



Raw Telemetry

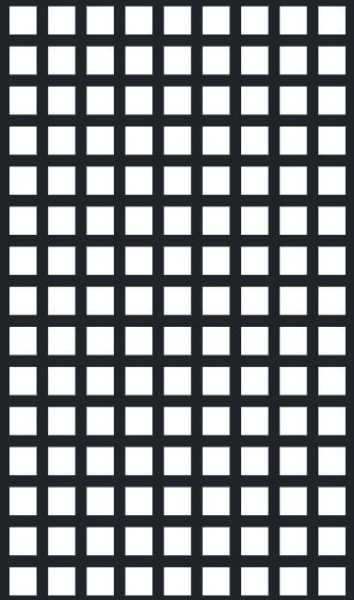
Intelligence & Hunts

12,723 detectors were evaluated against every piece of collected telemetry.

Retroactive hunts were performed for 4,342 newly identified indicators of compromise.

Your threat hunters performed 424 threat hunts with specific hypotheses in your environment.

9,033
Investigative leads



Suspicious Behavior

Key Takeaways

Red Canary's detection covers 373 of the 780 ATT&CK techniques.

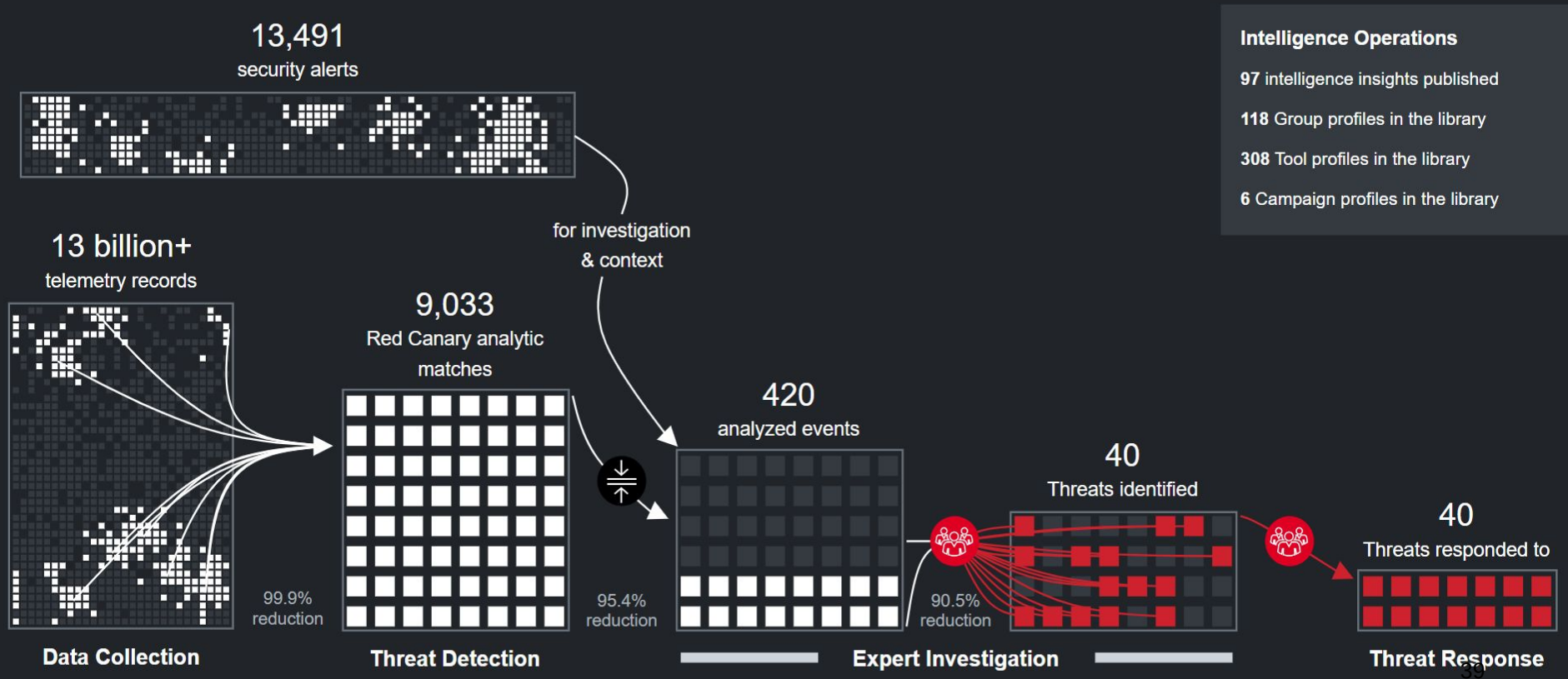
Coverage includes 100% of the top 20 most frequently used techniques.

During this period, our team of 98 detection and intelligence engineers created or modified 4,048 detectors.

Red Canary automatically hunts for new indicators of compromise when they are identified.

Background: Red Canary's Detection & Response by the Numbers

Custom range July 1, 2023 - June 30, 2024



Intelligence Operations

97 intelligence insights published

118 Group profiles in the library

308 Tool profiles in the library

6 Campaign profiles in the library

11 products integrated

27 TB data ingested

4,086 detection analytics applied

424 threat hunts performed

65 alerts associated with a Threat

13.4k alerts not associated with a Threat

6 high severity Threats

23 Red Canary unique Threats

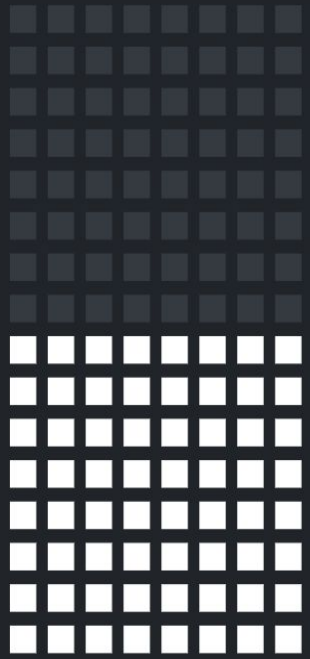
0 remediations by Red Canary

1k playbook actions triggered

Background: Expert Analysis & Investigation

Custom range July 1, 2023 - June 30, 2024

419
analyzed events



Correlated Activity

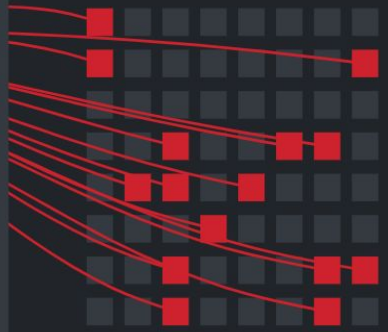
CIRT Investigation

The Red Canary CIRT investigated 419 potentially threatening events to determine if they were false positives or confirmed threats.

73% were false positives, most being legitimate software or users performing activity that is often associated with adversaries.

27% were true positives that identified threatening activity occurring in your environment.

40
threats



Confirmed Threats

Key Takeaways

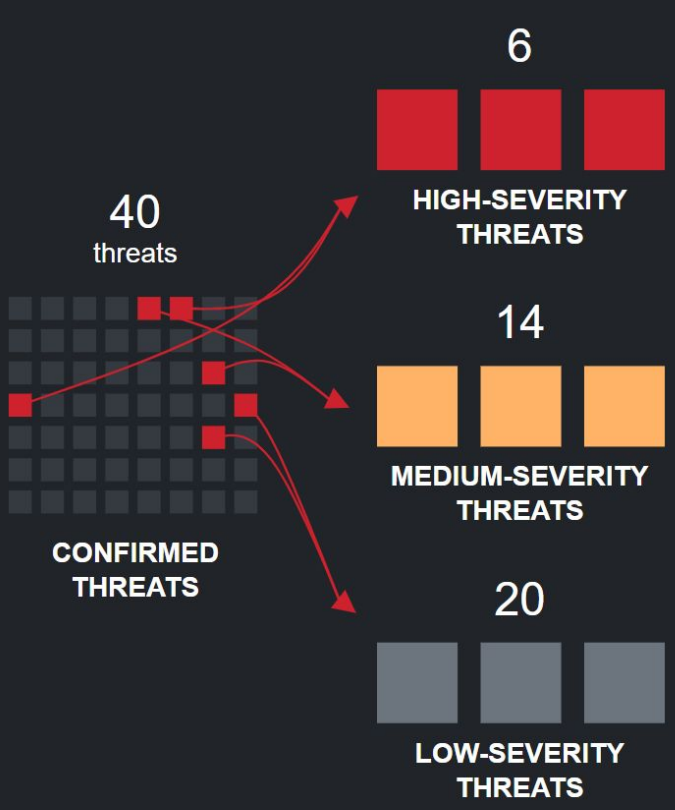
Red Canary's investigations saved your team from **more than 209 hours** of triage and investigation.

Red Canary investigated an average of **0.1 events / endpoint** during this period.

Each completed investigation results in additional intelligence that improves our detection accuracy, helping to defend your organization.

Background: Threats

Custom range July 1, 2023 - June 30, 2024



Key Takeaways

Red Canary's CIRT confirmed 20 medium and high severity threats:

- 5 were classified as Malicious Software of various types
- 15 were Suspicious Activity that required further review from your team

Confirmed threats were identified in a couple ways:

- 57% were identified by Red Canary's detection analytics
- The rest were identified using other forms of intelligence and detection techniques.

These threats involved a number of MITRE ATT&CK Tactics & Techniques:

- 7 tactics (led by Command and Control and Defense Evasion)
- 8 techniques (led by Remote Access Software and Email Hiding Rules)

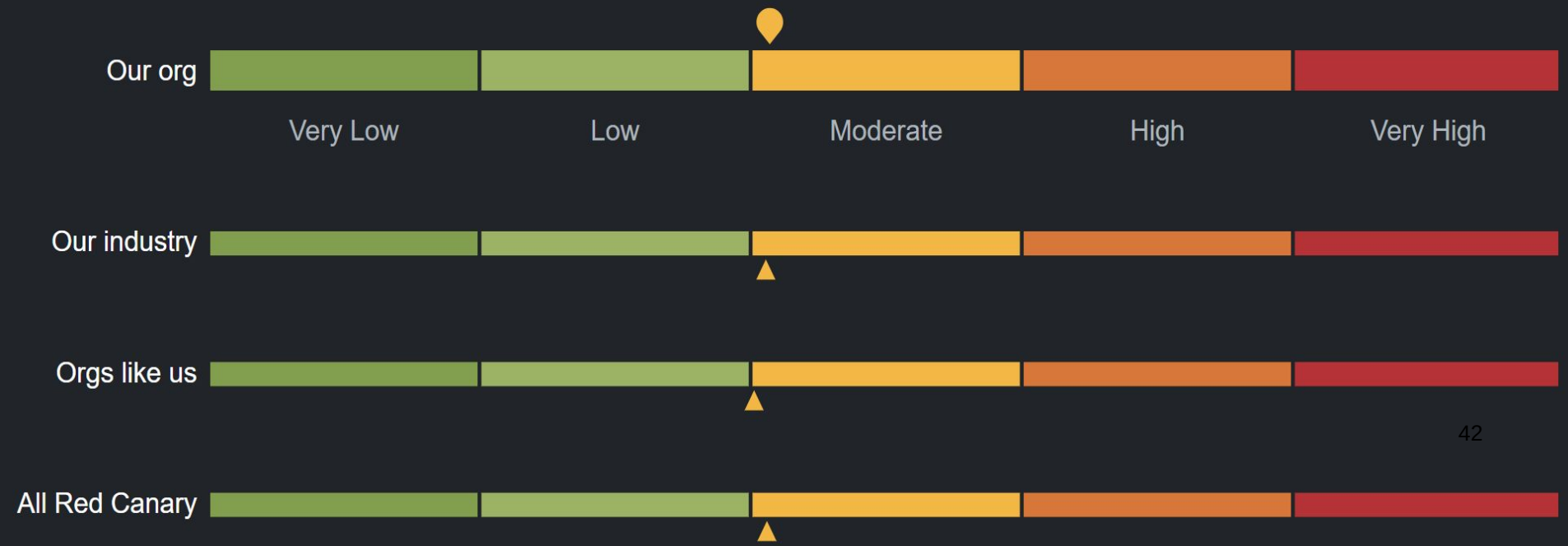
Confirmed threats contained 60 annotations from the Red Canary CIRT that provided context and guidance to your response teams.

Key Questions: How do we compare to other organizations?

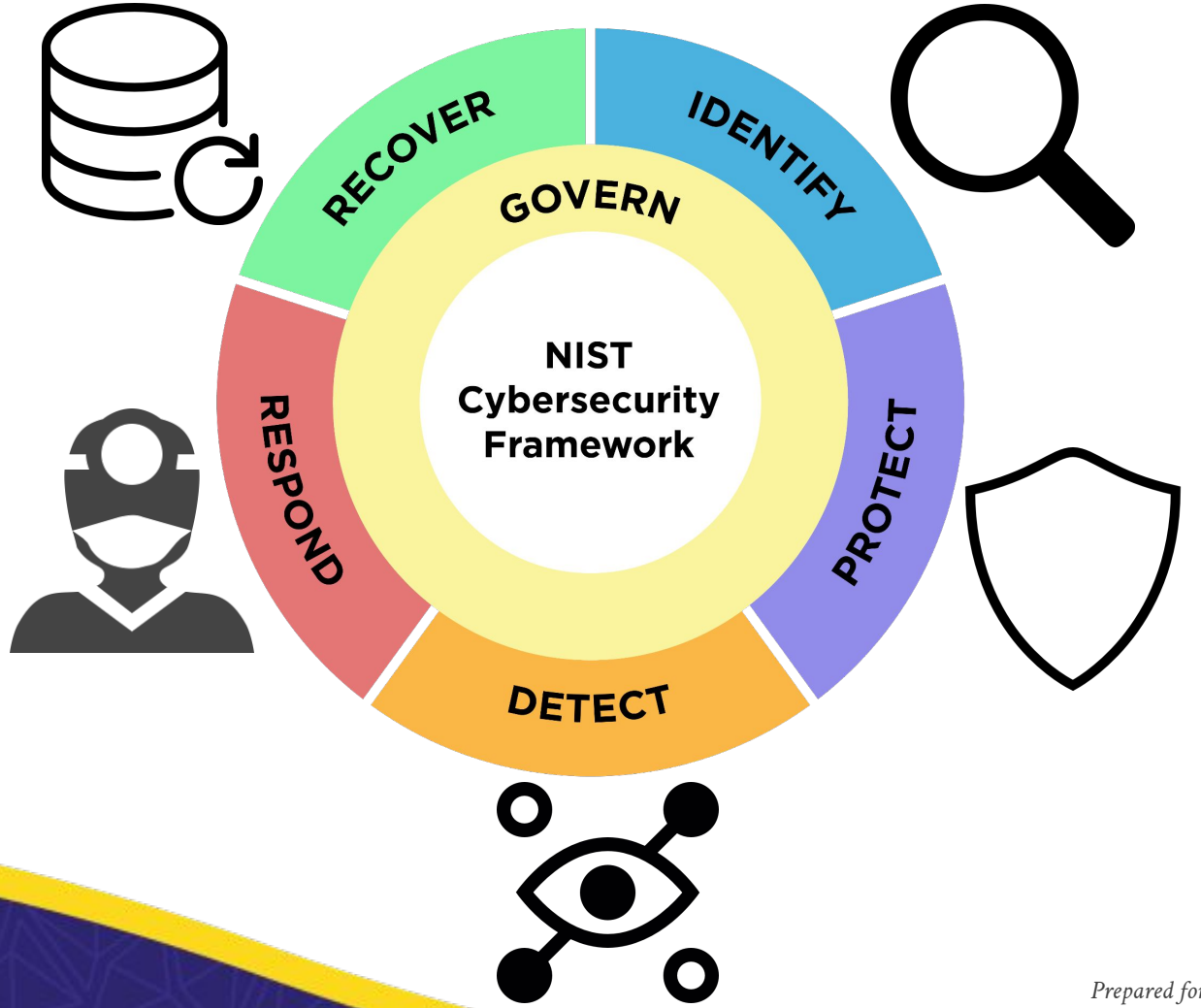
Trailing 6 months April 2, 2024 - October 2, 2024

Per-Endpoint Risk

Red Canary calculates per-endpoint risk by summing the total risk score from threats and dividing by the number of endpoints.



Cybersecurity work in Osseo Area Schools


RECOVER
IDENTIFY
GOVERN
NIST
Cybersecurity
Framework
RESPOND
PROTECT
DETECT

Focus

Training

Monitoring

Response

Digital Security Training

- Established annual digital security training for all employees
- Started tabletop exercises with district leadership
- Developing tabletop exercises for school leadership

Digital Security Monitoring

- Established monthly external scanning assessment
- Established quarterly phishing assessments
- Established Red Canary MDR
- Established Microsoft EDR

Digital Security Response

- Established a digital security plan
- Established digital security incident response plan
- Started district level continuity plans
- Started routine backup recovery testing
- Developing site level continuity plans

Questions?

FEDERAL BUREAU of INVESTIGATION

Internet Crime Report

2023

INTERNET CRIME COMPLAINT CENTER

CONTENTS

INTRODUCTION

Dear Reader,

Today's cyber landscape is threatened by a multitude of malicious actors who have the tools to conduct large-scale fraud schemes, hold our money and data for ransom, and endanger our national security. Profit-driven cybercriminals and nation-state adversaries alike have the capability to paralyze entire school systems, police departments, healthcare facilities, and individual private sector entities. The FBI continues to combat this evolving cyber threat. Our strategy focuses on building strong partnerships with the private sector; removing threats from US networks; pulling back the cloak of anonymity many of these actors hide behind; and hitting cybercriminals where it hurts: their wallets, including their virtual wallets.

Critical to the FBI's efforts is the Internet Crime Complaint Center (IC3). IC3 gives the public a direct way to report cybercrime to the FBI and enables us to collect data, advance investigations, and identify changes in the threat landscape. In 2023, IC3 received a record number of complaints from the American public: 880,418 complaints were registered, with potential losses exceeding $12.5 billion. This is a nearly 10% increase in complaints received, and it represents a 22% increase in losses suffered, compared to 2022. As impressive as these figures appear, we know they are conservative regarding cybercrime in 2023. Consider that when the FBI recently infiltrated the Hive ransomware group's infrastructure, we found that only about 20% of Hive's victims reported to law enforcement. More reporting from victims would mean superior insight for the FBI.

The past year, investment fraud was once again the costliest type of crime tracked by IC3. Losses to investment scams rose from $3.31 billion in 2022 to $4.57 billion in 2023—a 38% increase. The second-costliest type of crime was business e-mail compromise (BEC), with 21,489 complaints amounting to $2.9 billion in reported losses. Tech support scams, meanwhile, were the third-costliest type of crime tracked by IC3. Notably, different age groups tended to be impacted by different crimes. Victims 30 to 49 years old were the most likely group to report losses from investment fraud, while the elderly accounted for well over half of losses to tech support scams.

In 2023, ransomware incidents continued to be impactful and costly. After a brief downturn in 2022, ransomware incidents were again on the rise with over 2,825 complaints. This represents an increase of 18% from 2022. Reported losses rose 74%, from $34.3 million to $59.6 million. Cybercriminals continue to adjust their tactics, and the FBI has observed emerging ransomware trends, such as the deployment of multiple ransomware variants against the same victim and the use of data-destruction tactics to increase pressure on victims to negotiate.

Last year also saw notable achievements for law enforcement. The FBI's commitment to assisting cyber victims and fostering partnerships allowed for the continued success of IC3's Recovery Asset Team (RAT). Established in 2018, RAT streamlines communications with financial institutions and FBI field offices to facilitate the freezing of funds for victims. In 2023, IC3's RAT initiated the Financial Fraud Kill Chain (FFKC) on 3,008 incidents, with potential losses of $758.05 million. A monetary hold was placed on $538.39 million, representing a success rate of 71%.

As the cyber threat continues to evolve, the FBI remains appreciative of those who report cyber incidents to IC3. Information reported to the FBI helps advance our investigations. Your reporting is critical for our efforts to pursue adversaries, share intelligence with our partners, and protect your fellow citizens. Cybersecurity is the ultimate team sport, and we are in this fight together. The FBI is committed to fostering greater security in a digitally connected world, and we are eager to work with the American public to defeat cyber adversaries and bring criminals to justice.

Timothy Langan
Executive Assistant Director
Federal Bureau of Investigation

THE IC3

Today's FBI is an intelligence-driven and threat focused national security organization with both intelligence and law enforcement responsibilities. We are focused on protecting the American people from terrorism, espionage, cyber-attacks, and major criminal threats which are increasingly emanating from our digitally connected world. To do that, the FBI leverages the IC3 as a mechanism to gather intelligence on internet crime so that we can provide the public and our many partners with information, services, support, training, and leadership to stay ahead of the threat.

The IC3 was established in May 2000 to receive complaints crossing the spectrum of cyber matters, to include online fraud in its many forms including Intellectual Property Rights (IPR) matters, Computer Intrusions (Hacking), Economic Espionage (Theft of Trade Secrets), Online Extortion, International Money Laundering, Identity Theft, and a growing list of Internet-facilitated crimes. As of December 31, 2023, the IC3 has received over eight million complaints. The IC3's mission is to provide the public and our partners with a reliable and convenient reporting mechanism to submit information concerning suspected cyber-enabled criminal activity and to develop effective alliances with law enforcement and industry partners to help those who report. Information is analyzed and disseminated for investigative and intelligence purposes for law enforcement and public awareness.

The information submitted to the IC3 can be impactful in the individual complaints, but it is most impactful in the aggregate. That is, when the individual complaints are combined with other data, it allows the FBI to connect complaints, investigate reported crimes, track trends and threats, and, in some cases, even freeze stolen funds. Just as importantly, the IC3 shares reports of crime throughout its vast network of FBI field offices and law enforcement partners, strengthening our nation's collective response both locally and nationally.

To promote public awareness and as part of its prevention mission, the IC3 aggregates the submitted data and produces an annual report on the trends impacting the public as well as routinely providing intelligence reports about trends. The success of these efforts is directly related to the quality of the data submitted by the public through the www.ic3.gov interface. Their efforts help the IC3, and the FBI better protect their fellow citizens.

THE IC3'S ROLE IN COMBATTING CYBER CRIME[1]

[1] Accessibility description: Image lists the IC3's primary functions including partnering with private sector and with local, state, federal, and international agencies: hosting a reporting portal at www.ic3.gov; providing a central hub to alert the public to threats; Perform Analysis, Complaint Referrals, and Asset Recovery; and hosting a remote access database for all law enforcement via the FBI's LEEP website.

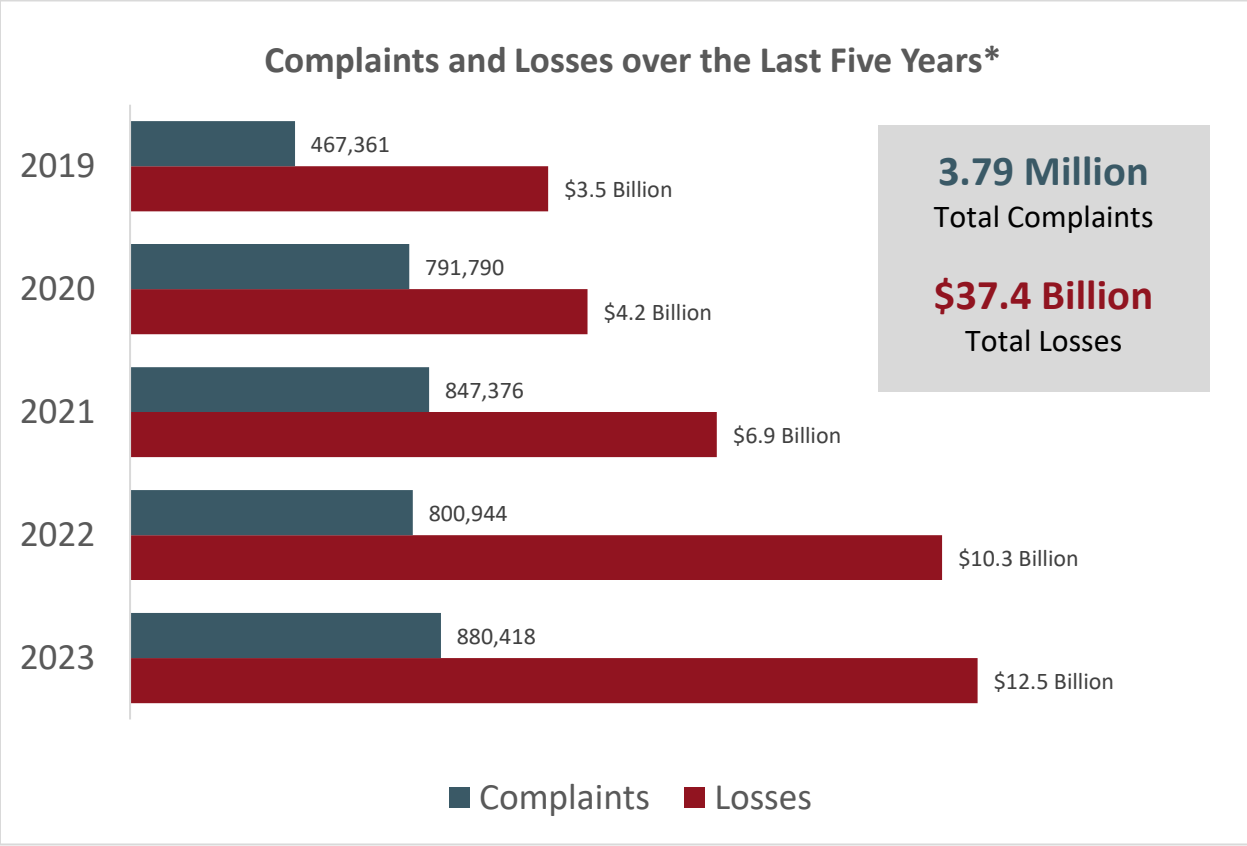
IC3 CORE FUNCTIONS[2]

[2] Accessibility description: Image contains icons with the core functions. Core functions - Collection, Analysis, Public Awareness, and Referrals - are listed in individual blocks as components of an ongoing process.

IC3 COMPLAINT STATISTICS

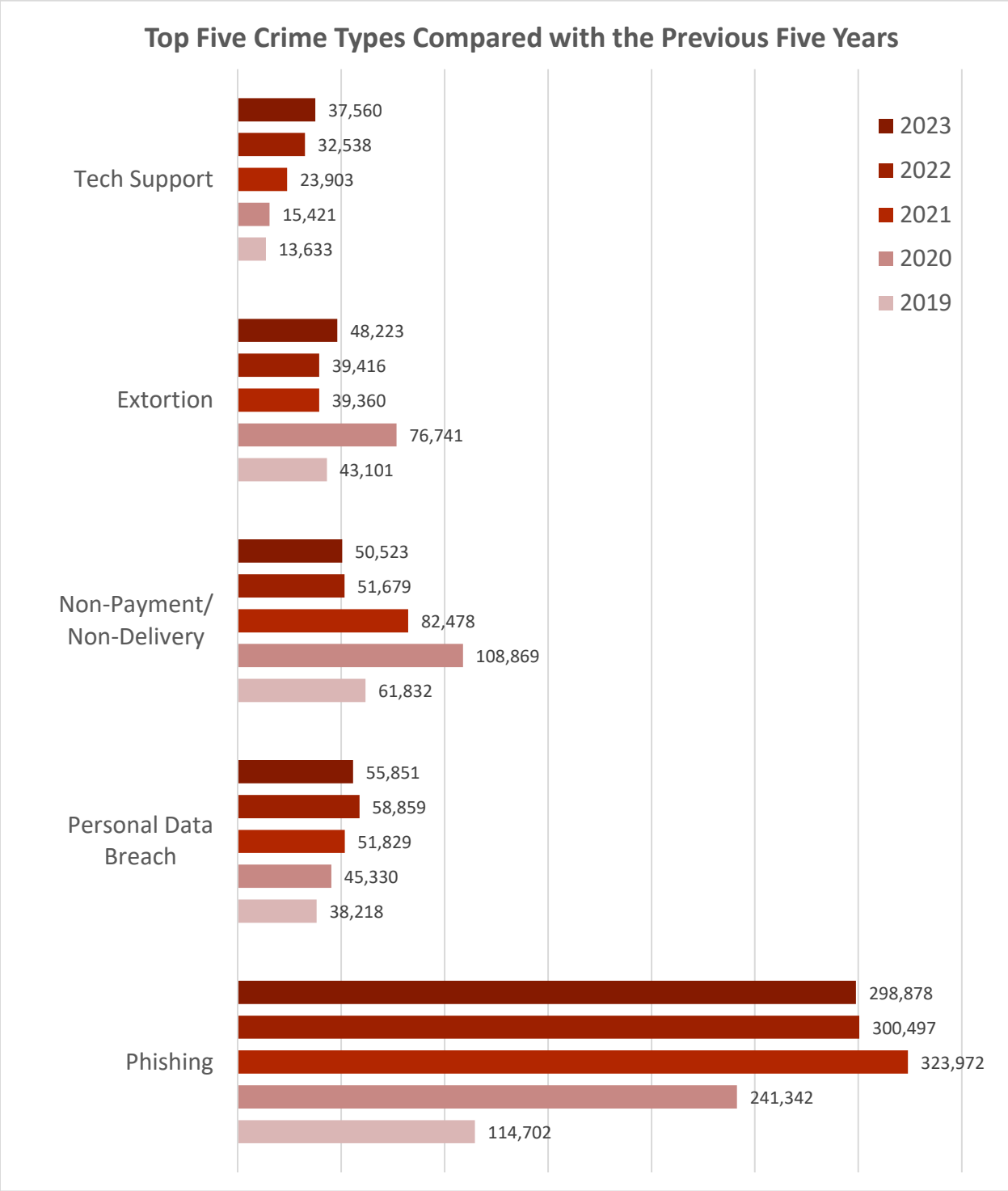
LAST FIVE YEARS

Over the last five years, the IC3 has received an average of 758,000 complaints per year. These complaints address a wide array of Internet scams affecting individuals across the globe.[3]



[3] Accessibility description: Chart includes yearly and aggregate data for complaints and losses over the years 2019 to 2023. Over this time, the IC3 received a total of 3.79 million complaints, reporting a loss of $37.5 billion. * Please see Appendix B for more information regarding IC3 data.

TOP FIVE CRIME TYPE COMPARISON[4]

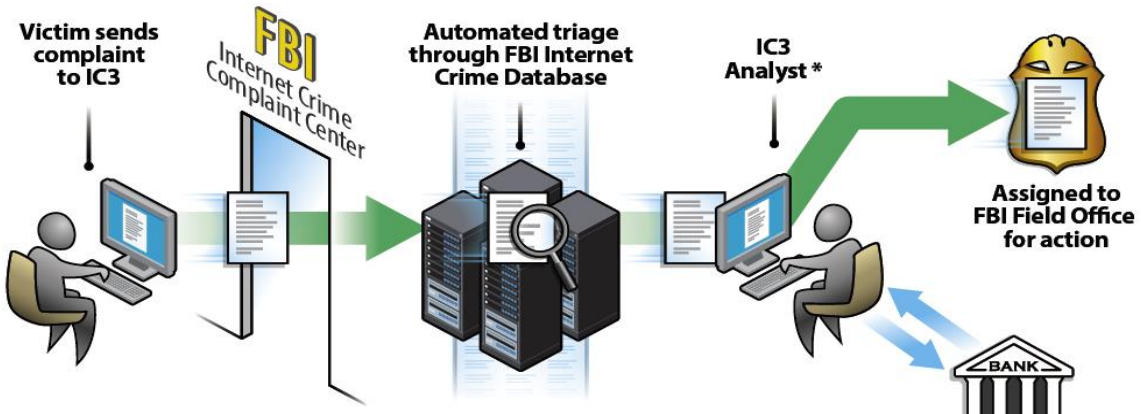


[4] Accessibility description: Chart includes a loss comparison for the top five reported crime types for the years of 2019 to 2023.

THE IC3 RECOVERY ASSET TEAM (RAT)

The Internet Crime Complaint Center's Recovery Asset Team (RAT) was established in February 2018 to streamline communication with financial institutions and assist FBI field offices with the freezing of funds for those who made transfers to domestic accounts under fraudulent pretenses.

RAT Process[5]



* If criteria are met, transaction details are forwarded to the identified point of contact at the recipient bank to notify of fraudulent activity and request freezing of the account. Once response is received from the recipient bank, RAT contacts the appropriate FBI field office(s).

The RAT functions as a liaison between law enforcement and financial institutions supporting statistical and investigative analysis.

Goals of RAT-Financial Institution Partnership

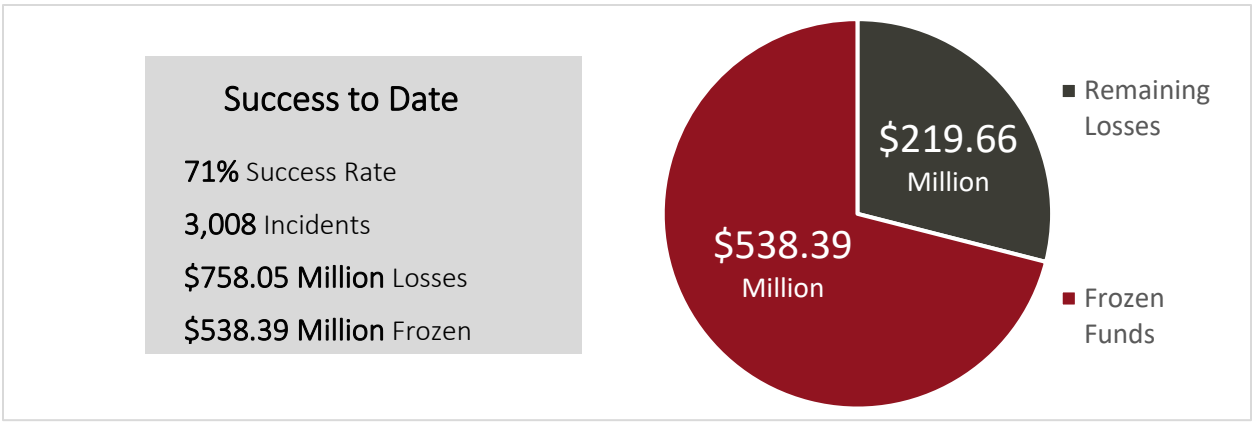
- Assist in the identification of potentially fraudulent accounts across the sector.
- Remain at the forefront of emerging trends among financial fraud schemes.
- Foster a symbiotic relationship in which information is appropriately shared.

Guidance for Complainants who send Wire Transfers

- Contact the originating financial institution as soon as fraud is recognized to request a recall or reversal and a Hold Harmless Letter or Letter of Indemnity.
- File a detailed complaint with www.ic3.gov. It is vital the complaint contain all required data in provided fields, including banking information.
- Never make any payment changes without verifying the change with the intended recipient; verify email addresses are accurate when checking email on a cell phone or other mobile device.

[5] Accessibility description: Image shows the different stages of a complaint in the RAT process.

RAT SUCCESSES[6]



The IC3 RAT has proven to be a valuable resource for field offices and victims. The following are two examples of the RAT's successful contributions to investigative and recovery efforts:

New York

In March of 2023, the IC3 received a complaint filed by a critical infrastructure construction project entity located in New York, New York area of a $50,000,000 loss due to a BEC incident. The RAT immediately sent the Financial Fraud Kill Chain (FFKC) request to the recipient financial institution and was advised that $44,936,460 was frozen in the account. Second-hop information was provided by the recipient financial institution, and the RAT pursued the secondary wires to two additional recipient financial institutions. FFKC responses from the second wires reported a frozen amount of an additional $1,008,526.

Connecticut

In March 2023, the IC3 received a complaint filed by an individual located in the Stamford, Connecticut area of a BEC related to a real estate transaction. The individual was in the process of purchasing a home and received a spoofed email from their supposed attorney instructing them to wire $426,000.00 to a financial institution to finalize the closing. Two days after the wire was initiated, it was realized the instructions came from a spoofed email. Upon notification, the IC3 RAT immediately initiated the FFKC process to freeze the fraudulent recipient financial bank account. Collaboration with the domestic recipient financial institution and the local police department confirmed $425,000.00 was frozen and returned to the individual which enabled them to complete the real estate transaction.

[6] Accessibility description: Image shows Success to Date to include 71% Success Rate; 3,008 Incidents; $758.05 Million in Losses; and $538.39 Million Frozen.

2023 OVERVIEW

BUSINESS EMAIL COMPROMISE (BEC)

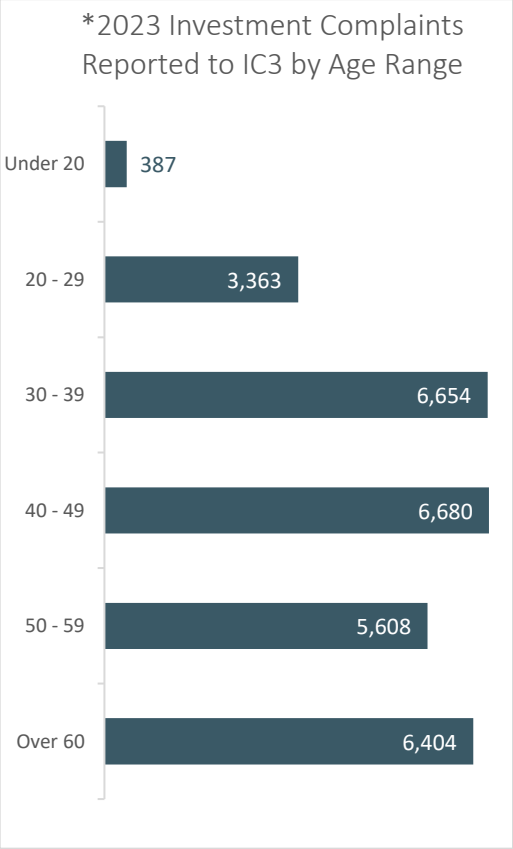
In 2023, the IC3 received 21,489 BEC complaints with adjusted losses over 2.9 billion. BEC is a sophisticated scam targeting both businesses and individuals performing transfers of funds. The scam is frequently carried out when a subject compromises legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.

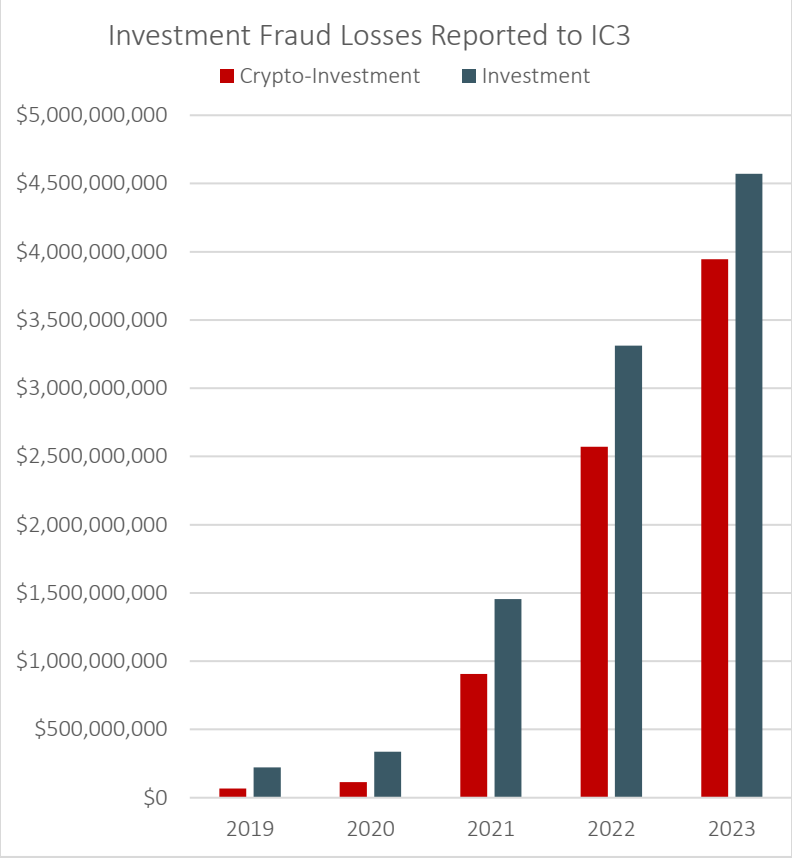
These BEC schemes historically involved compromised vendor emails, requests for W-2 information, targeting of the real estate sector, and fraudulent requests for large amounts of gift cards. More recently, the IC3 data suggests fraudsters are increasingly using custodial accounts held at financial institutions for cryptocurrency exchanges or third-party payment processors, or having targeted individuals send funds directly to these platforms where funds are quickly dispersed.

With these increased tactics of funds going directly to cryptocurrency platforms and third-party payment processors or through a custodial account held at a financial institution, it emphasizes the importance of leveraging two-factor or multi-factor authentication as an additional security layer. Procedures should be put in place to verify payments and purchase requests outside of email communication and can include direct phone calls but to a known verified number and not relying on information or phone numbers included in the email communication. Other best practices include carefully examining the email address, URL, and spelling used in any correspondence and not clicking on anything in an unsolicited email or text message asking you to update or verify account information.

INVESTMENT

In 2023, the losses reported due to Investment scams became the most of any crime type tracked by the IC3. Investment fraud losses rose from $3.31 billion in 2022 to $4.57 billion in 2023, a 38% increase. Within these numbers, investment fraud with a reference to cryptocurrency rose from $2.57 billion in 2022 to $3.96 billion in 2023, an increase of 53%. These scams are designed to entice those targeted with the promise of lucrative returns on their investments. [7],[8]





**Does not include complainants that did not provide an age range.*

IC3 publications in 2023 Related to Investment Fraud

- The FBI Warns of a Spike in Cryptocurrency Investment Schemes
- FBI Guidance for Cryptocurrency Scam Victims
- Increase in Companies Falsely Claiming an Ability to Recover Funds Lost in Cryptocurrency Investment Scams
- Criminals Pose as Non-Fungible Token (NFT) Developers to Target Internet Users with an Interest in NFT Acquisition

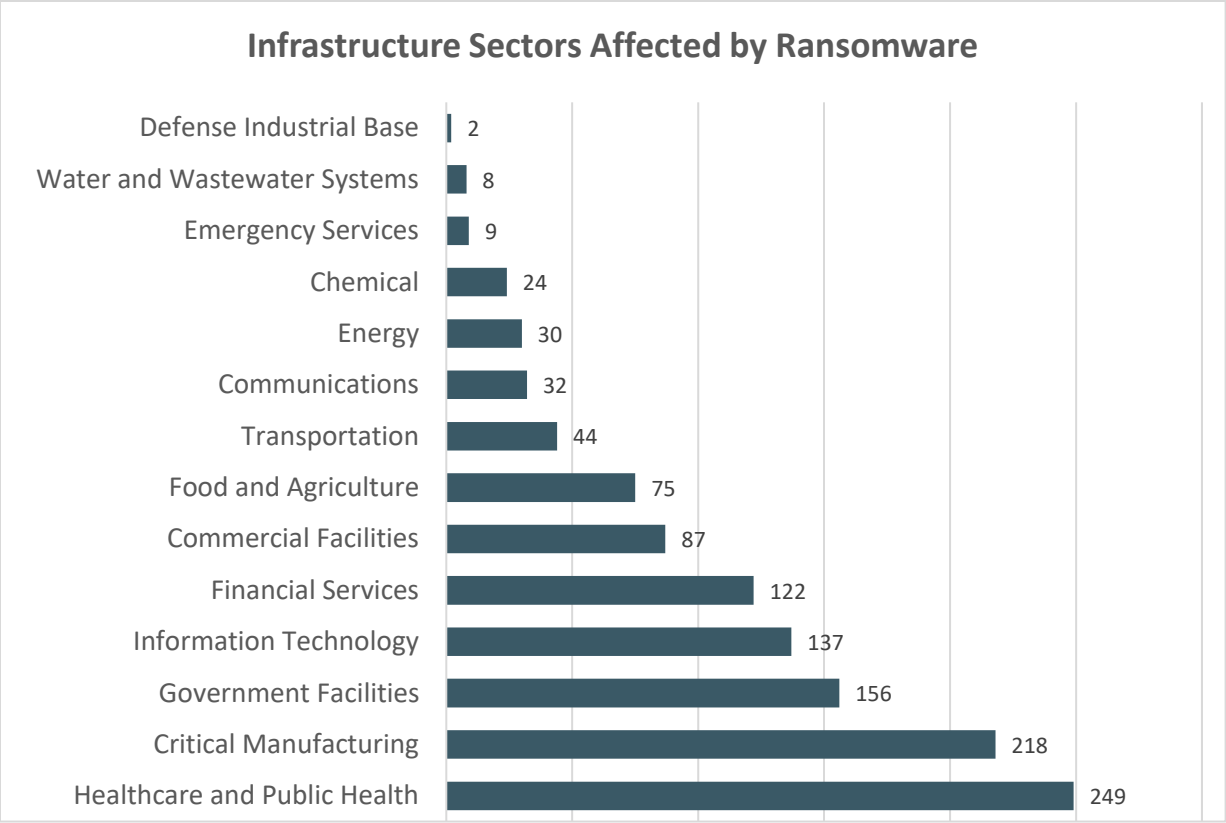
[7] Accessibility description: 2023 Investment Complaints Reported to IC3 by Age Range.
[8] Accessibility description: Chart shows Investment Fraud Losses Reported to the IC3 by Year for 2019 to 2023.

RANSOMWARE

In 2023, the IC3 received 2,825 complaints identified as ransomware with adjusted losses of more than $59.6 million. Ransomware is a type of malicious software, or malware, that encrypts data on a computer, making it unusable. In addition to encrypting the network, the cyber-criminal will often steal data off the system and hold that data hostage until the ransom is paid. If the ransom is not paid, the entity's data remains unavailable.

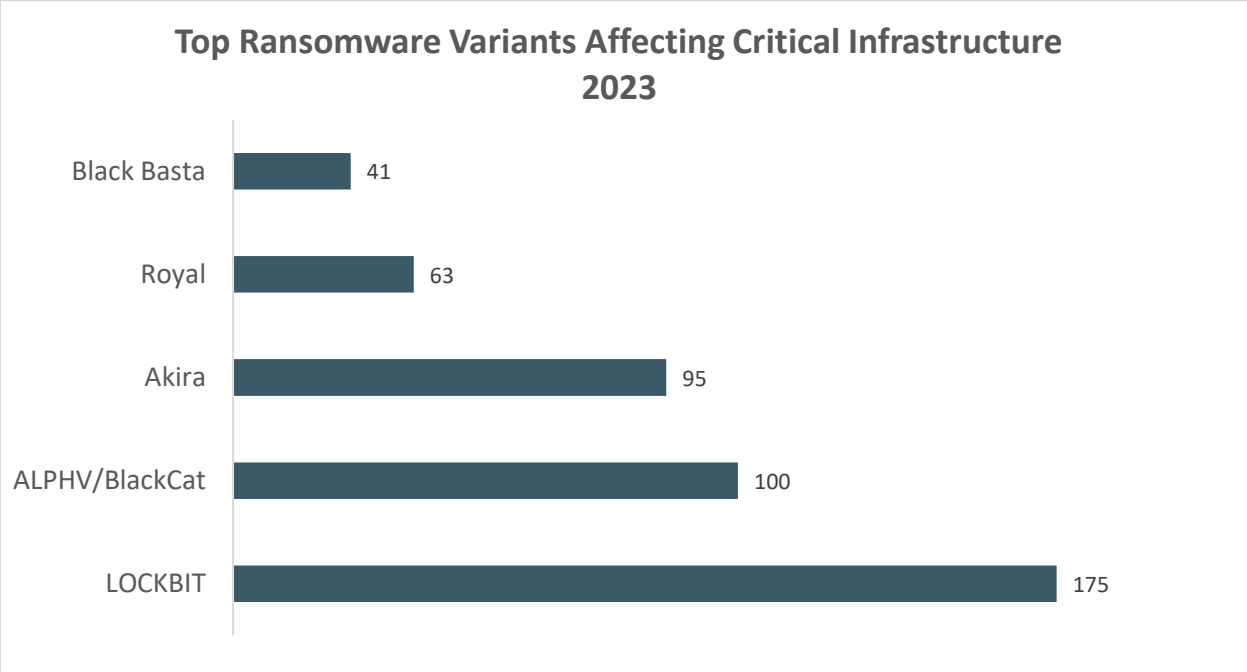
Ransomware and Critical Infrastructure Sectors

The IC3 received 1,193 complaints from organizations belonging to a critical infrastructure sector that were affected by a ransomware attack. Of the 16 critical infrastructure sectors, IC3 reporting indicated 14 sectors had at least 1 member that fell to a ransomware attack in 2023.[9]



[9] Accessibility description: Chart shows Infrastructure Sectors Affected by Ransomware. Healthcare and Public Health was highest with 249; followed by Critical Manufacturing 218; Government Facilities 156; Information Technology 137; Financial Services 122; Commercial Facilities 87; Food and Agriculture 75; Transportation 44; Communications 32; Energy 30; Chemical 24; Emergency Services 9; Water and Wastewater Systems 8; Defense Industrial Base 2.

The five top ransomware variants reported to the IC3 that affected a member of a critical infrastructure sector were Lockbit, ALPHV/Blackcat, Akira, Royal, and Black Basta.[10]



Incident reporting

Ransomware infections impact individual users and businesses regardless of size or industry by causing service disruptions, financial loss, and in some cases, permanent loss of valuable data. While ransomware infection statistics are often highlighted in the media and by computer security companies, it has been challenging for the FBI to ascertain the true number of ransomware victims as many infections go unreported to law enforcement. By reporting the incident, the FBI may be able to provide information on decryption, recover stolen data, possibly seize/recover ransom payments, and gain insight on adversary tactics. Ultimately, the information you provide will lead us to bring the perpetrators to justice.

The FBI does not encourage paying a ransom to criminal actors. Paying a ransom may embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities. Paying the ransom also does not guarantee that an entity's files will be recovered. Regardless of whether you or your organization decided to pay the ransom, the FBI urges you to report ransomware incidents to the IC3. Doing so provides investigators with the critical information they need to track ransomware attackers, hold them accountable under U.S. law, and prevent future attacks.

[10] Accessibility description: Chart shows Top Ransomware Variants Affecting Critical Infrastructure 2023 Incidents. Lockbit, ALPHV/Blackcat, Akira, Royal, and Black Basta.

TECH/CUSTOMER SUPPORT AND GOVERNMENT IMPERSONATION [11]

Impersonation scams defraud thousands of individuals each year. Two categories of fraud reported to IC3, Tech/Customer Support and Government Impersonation, are responsible for over $1.3 billion in losses.

	Complaints	Losses	Trend
Government Impersonation	14,190	$394,050,518	▲63%
Tech and Customer Support	37,560	$924,512,658	▲15%
TOTAL	51,750	$1,318,563,176	

Call centers overwhelmingly target older adults, with devastating effects. Almost half the complainants report to be Over 60 (40%), and experience 58% of the losses (over $770 million).

Investigative Success Stories

FBI Knoxville Cyber Squad: The initial complaint received from IC3 spearheaded the investigation by identifying the main subjects, Ankur Khemani, and the Sterks, a family based in Iowa. Khemani and his co-conspirators duped thousands of victims into believing their computers were infected with malicious malware. The resulting investigation grew from 50 initial IC3 reports to over 14,000 victims with over $4 million in losses. On September 28, 2023, Khemani was sentenced in Knoxville federal court to 75 months for orchestrating a fraudulent computer technical support ring based in India. On December 20, 2023, Marilyn Sterk, along with her daughter Teresa Sterk, and daughter-in-law Jennifer Sterk, were sentenced in Knoxville federal court for their involvement in a tech support scheme. The Sterks opened over 30 bank accounts to launder money obtained from victims of an India-based tech support scam. Marilyn was sentenced to 30 months in prison, while her daughters received three years of probation.

FBI, Legat New Delhi, Washington Field: Since 2022, the DOJ, the FBI Legal Attaché New Delhi, the Washington Field Office (WFO), and IC3 have collaborated with law enforcement in India, such as the Central Bureau of Investigation in New Delhi and local Indian states, to combat cyber-enabled financial crimes and transnational call center fraud. In 2023, Indian law enforcement accomplished multiple call center raids, disruptions, seizures, and arrests of the individuals alleged to be involved in perpetrating these crimes. The FBI enabled 26 arrests through 13 joint operations with Indian authorities. WFO conducted hundreds of interviews and continues to support Indian law enforcement efforts and prosecution of call centers perpetrating these frauds.

IC3 publications in 2023 Related to Tech/Customer Support and Government Impersonation

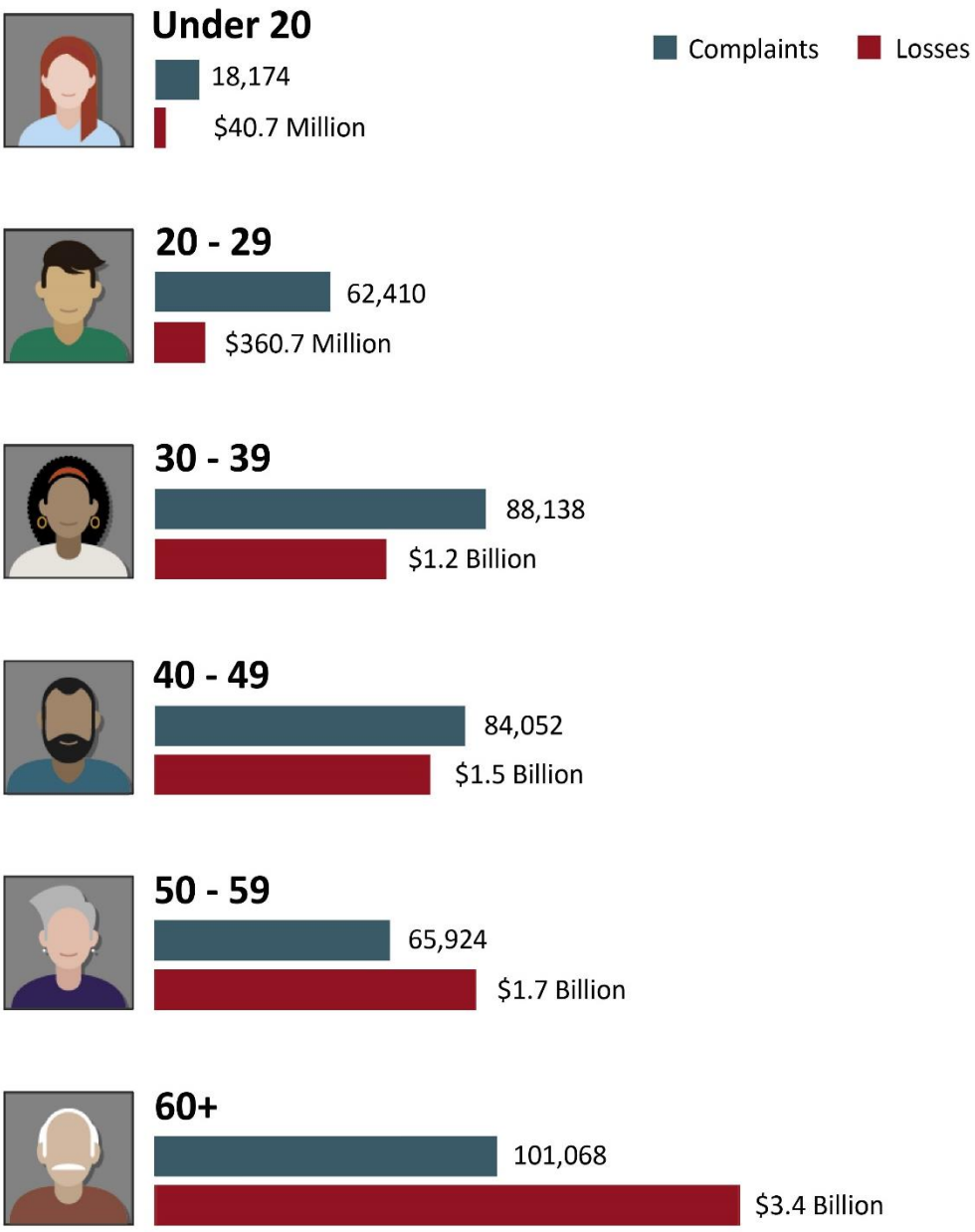
- "Phantom Hacker" Scams Target Senior Citizens and Result in Victims Losing their Life Savings
- Increase in Tech Support Scams Targeting Older Adults and Directing Victims to Send Cash through Shipping Companies
- Criminals Pose as Chinese Authorities to Target US-based Chinese Community (简体中文版) (繁體中文版)

[11] Accessibility description: Chart shows number of Government Impersonation and Tech and Customer Support complainants and losses for 2023.

IC3 BY THE NUMBERS[12]

[12] Accessibility description: Image depicts key statistics regarding complaints and losses. Total losses of $12.5 billion were reported in 2023. The total number of complaints received since the year 2000 is over 8 million. The IC3 has received approximately 758,000 complaints per year on average over the last five years, or more than 2,412 complaints per day.

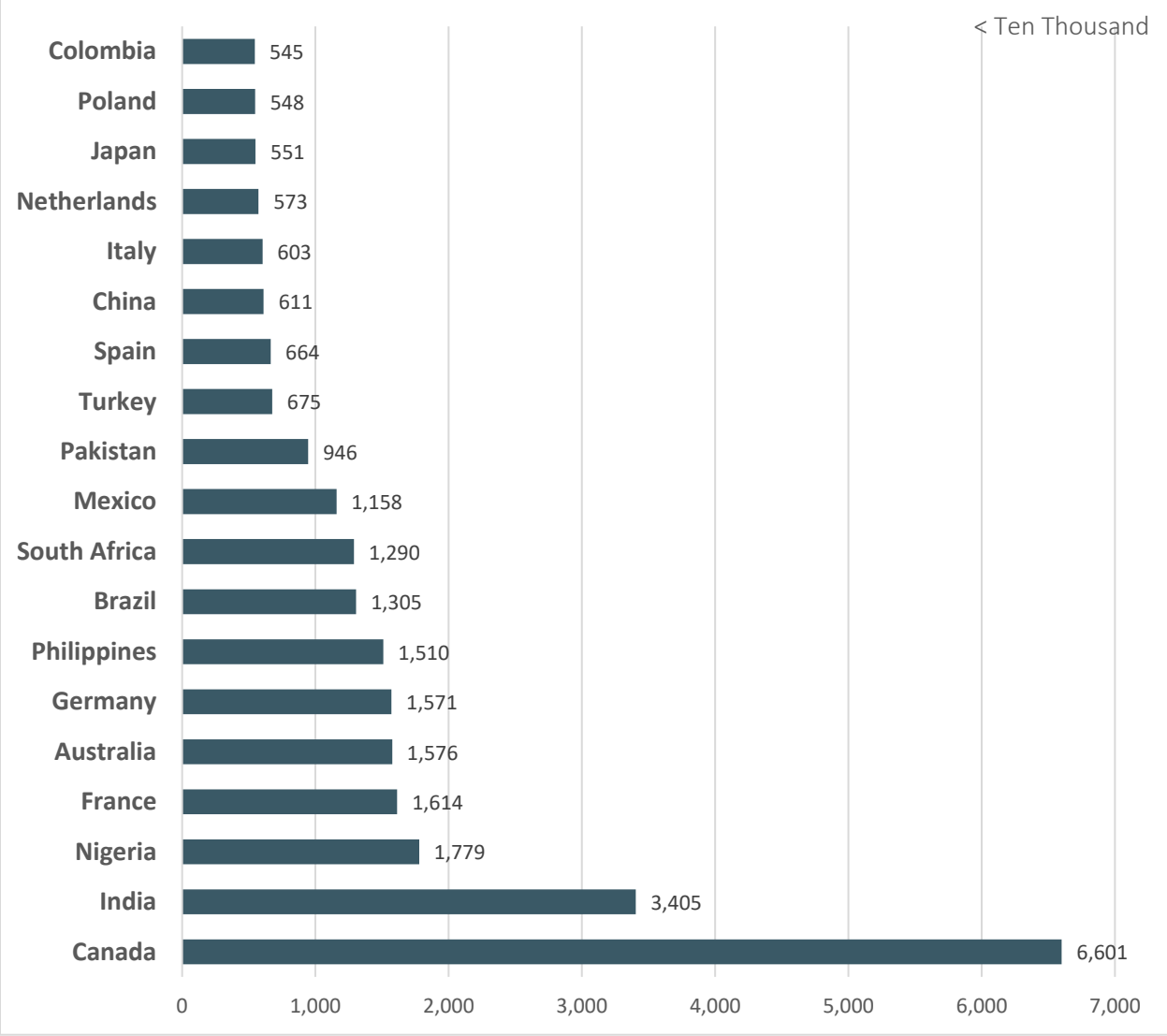
2023 - COMPLAINANTS BY AGE GROUP [13]

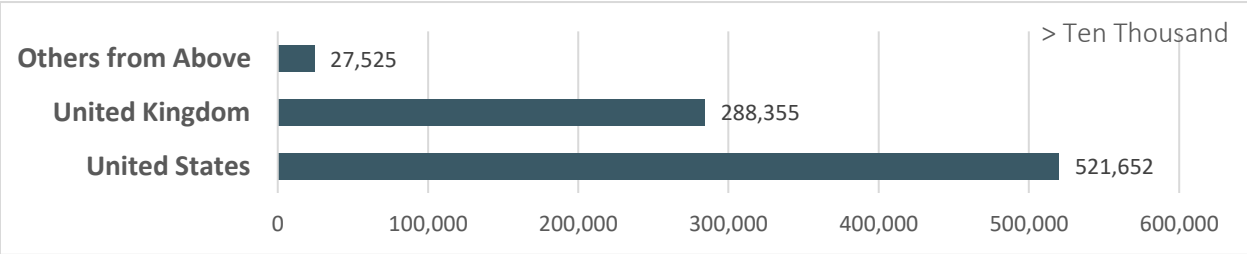


[13] Not all complaints include an associated age range—those without this information are excluded from this table. Please see Appendix B for more information regarding IC3 data. Accessibility description: Chart shows number of Complaints and Losses by Age Group. Under 20 18,174 Complaints, $40.7 Million losses; 20-29 62,410 Complaints, $360.7 Million losses; 30-39 88,138 Complaints, $1.2 Billion losses; 40-49 84,052 Complaints, $1.5 Billion losses; 50-59 65,924 Complaints, $1.7 Billion losses; 60+ 101,068 Complaints, $3.4 Billion losses.

2023 - TOP 20 INTERNATIONAL COMPLAINT COUNTRIES [14]

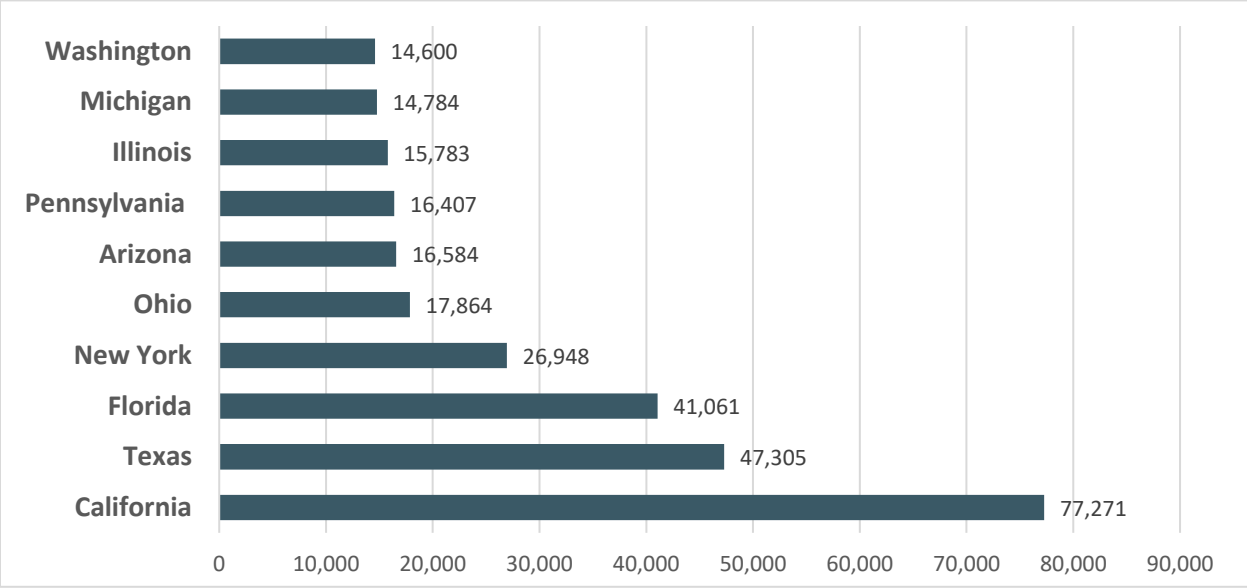
Compared to the United States



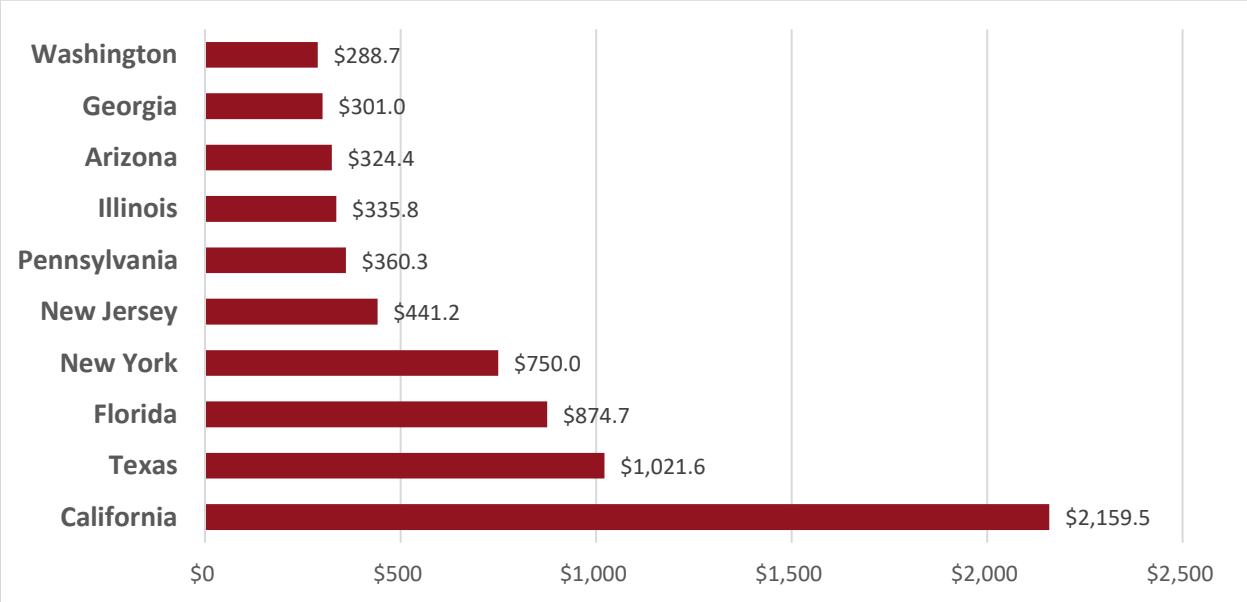


[14] Accessibility description: the charts list the top 20 countries by number of total complaints as compared to the United States and United Kingdom. The specific number of complaints for each country are listed in ascending order to the right of the graph. Please see Appendix B for more information regarding IC3 data.

2023 - TOP 10 STATES BY NUMBER OF COMPLAINTS [15]



2023 - TOP 10 STATES BY LOSS (IN MILLIONS) [16]



[15] Accessibility description: Chart depicts the top 10 states based on number of complaints are labeled. These include California, Texas, Florida, New York, Ohio, Arizona, Pennsylvania, Illinois, Michigan, and Washington. Please see Appendix B for more information regarding IC3 data.

[16] Accessibility description: Chart depicts the top 10 states based on reported losses are labeled. These include California, Texas, Florida, New York, New Jersey, Pennsylvania, Illinois, Arizona, Georgia, and Washington. Please see Appendix B for more information regarding IC3 data.

2023 CRIME TYPES

By Complaint Count			
Crime Type	*Complaints*	*Crime Type*	*Complaints*
Phishing/Spoofing	298,878	Other	8,808
Personal Data Breach	55,851	Advanced Fee	8,045
Non-payment/Non-Delivery	50,523	Lottery/Sweepstakes/Inheritance	4,168
Extortion	48,223	Overpayment	4,144
Investment	39,570	Data Breach	3,727
Tech Support	37,560	Ransomware	2,825
BEC	21,489	Crimes Against Children	2,361
Identity Theft	19,778	Threats of Violence	1,697
Confidence/Romance	17,823	IPR/Copyright and Counterfeit	1,498
Employment	15,443	SIM Swap	1,075
Government Impersonation	14,190	Malware	659
Credit Card/Check Fraud	13,718	Botnet	540
Harassment/Stalking	9,587		
Real Estate	9,521		
*Descriptors**			
Cryptocurrency	43,653	Cryptocurrency Wallet	25,815

*These descriptors relate to the medium or tool used to facilitate the crime and are used by the IC3 for tracking purposes only. They are available as descriptors only after another crime type has been selected. Please see Appendix B for more information regarding IC3 data.

2023 CRIME TYPES continued

By Complaint Loss

Crime Type	*Loss*	*Crime Type*	*Loss*
Investment	$4,570,275,683	Extortion	$74,821,835
BEC	$2,946,830,270	Employment	$70,234,079
Tech Support	$924,512,658	Ransomware*	$59,641,384
Personal Data Breach	$744,219,879	SIM Swap	$48,798,103
Confidence/Romance	$652,544,805	Overpayment	$27,955,195
Data Breach	$534,397,222	Botnet	$22,422,708
Government Impersonation	$394,050,518	Phishing/Spoofing	$18,728,550
Non-payment/Non-Delivery	$309,648,416	Threats of Violence	$13,531,178
Other	$240,053,059	Harassment/Stalking	$9,677,332
Credit Card/Check Fraud	$173,627,614	IPR/Copyright and Counterfeit	$7,555,329
Real Estate	$145,243,348	Crimes Against Children	$2,031,485
Advanced Fee	$134,516,577	Malware	$1,213,317
Identity Theft	$126,203,809		
Lottery/Sweepstakes/Inheritance	$94,502,836		

*Descriptors***			
Cryptocurrency	$3,809,090,856	Cryptocurrency Wallet	$1,778,399,729

*Regarding ransomware adjusted losses, this number does not include estimates of lost business, time, wages, files, or equipment, or any third-party remediation services acquired by an entity. In some cases, entities do not report any loss amount to the FBI, thereby creating an artificially low overall ransomware loss rate. Lastly, the number only represents what entities report to the FBI via the IC3 and does not account for the entity direct reporting to FBI field offices/agents.

**These descriptors relate to the medium or tool used to facilitate the crime and are used by the IC3 for tracking purposes only. They are available only after another crime type has been selected. Please see Appendix B for more information regarding IC3 data.

LAST-THREE-YEAR COMPLAINT COUNT COMPARISON

By Complaint Count						▼ ▲ = Trend from previous Year
Crime Type	***2023***		*2022*		*2021*	
Advanced Fee	8,045	▼	11,264	▲	11,034	▼
BEC	21,489	▼	21,832	▲	19,954	▲
Botnet	540	▼	568		N/A	
Confidence Fraud/Romance	17,823	▼	19,021	▼	24,299	▲
Credit Card/Check Fraud	13,718	▼	22,985	▲	16,750	▼
Crimes Against Children	2,361	▼	2,587	▲	2,167	▼
Data Breach	3,727	▲	2,795	▲	1,287	▼
Employment	15,443	▲	14,946	▼	15,253	▼
Extortion	48,223	▲	39,416	▲	39,360	▼
Government Impersonation	14,190	▲	11,554	▲	11,335	▼
Harassment/Stalking	9,587	▼	11,779		N/A	
Identity Theft	19,778	▼	27,922	▼	51,629	▲
Investment	39,570	▲	30,529	▲	20,561	▲
IPR/Copyright and Counterfeit	1,498	▼	2,183	▼	4,270	▲
Lottery/Sweepstakes/Inheritance	4,168	▼	5,650	▼	5,991	▼
Malware	659	▼	762	▼	810	▼
Non-Payment/Non-Delivery	50,523	▼	51,679	▼	82,478	▼
Other	8,808	▼	9,966	▼	12,346	▲
Overpayment	4,144	▼	6,183	▲	6,108	▼
Personal Data Breach	55,851	▼	58,859	▲	51,829	▲
Phishing/Spoofing	298,878	▼	321,136	▼	342,494	▲
Ransomware	2,825	▲	2,385	▼	3,729	▲
Real Estate	9,521	▼	11,727	▲	11,578	▼
SIM Swap	1,075	▼	2,026		N/A	
Tech Support	37,560	▲	32,538	▲	23,903	▲
Threats of Violence	1,697	▼	2,224		N/A	

LAST-THREE-YEAR COMPLAINT LOSS COMPARISON

By Complaint Loss	▼ ▲ = Trend from previous Year		
Crime Type	***2023***	*2022*	*2021*
Advanced Fee	$134,516,577 ▲	$104,325,444 ▲	$98,694,137 ▲
BEC	$2,946,830,270 ▲	$2,742,354,049 ▲	$2,395,953,296 ▲
Botnet	$22,422,708 ▲	$17,099,378 ▲	N/A
Confidence Fraud/Romance	$652,544,805 ▼	$735,882,192 ▼	$956,039,739 ▲
Credit Card/Check Fraud	$173,627,614 ▼	264,148,905 ▲	$172,998,385 ▲
Crimes Against Children	$2,031,485 ▲	$577,464 ▲	$198,950 ▼
Data Breach	$534,397,222 ▲	$459,321,859 ▲	$151,568,225 ▲
Employment	$70,234,079 ▲	$52,204,269 ▲	$47,231,023 ▼
Extortion	$74,821,835 ▲	$54,335,128 ▼	$60,577,741 ▼
Government Impersonation	$394,050,518 ▲	$240,553,091 ▲	$142,643,253 ▲
Harassment/Stalking	$9,677,332 ▲	$5,621,402	N/A
Identity Theft	$126,203,809 ▼	189,205,793 ▼	$278,267,918 ▲
Investment	$4,570,275,683 ▲	$3,311,742,206 ▲	$1,455,943,193 ▲
IPR/Copyright and Counterfeit	$7,555,329 ▲	$4,591,177 ▼	$16,365,011 ▲
Lottery/Sweepstakes/Inheritance	$94,502,836 ▲	$83,602,376 ▲	$71,289,089 ▲
Malware	$1,213,317 ▼	$9,326,482 ▲	$5,596,889 ▼
Non-Payment/Non-Delivery	$309,648,416 ▲	$281,770,073 ▼	$337,493,071 ▲
Other	$240,053,059 ▲	$117,686,789 ▲	$75,837,524 ▼
Overpayment	$27,955,195 ▼	$38,335,772 ▲	$33,407,671 ▼
Personal Data Breach	$744,219,879 ▲	$742,438,136 ▲	$517,021,289 ▲
Phishing/Spoofing	$18,728,550 ▼	$160,015,411 ▲	$126,383,513 ▼
Ransomware	$59,641,384 ▲	$34,353,237 ▼	$49,207,908 ▲
Real Estate	$145,243,348 ▼	$396,932,821 ▲	$350,328,166 ▲
SIM Swap	$48,798,103 ▼	$72,652,571	N/A
Tech Support	$924,512,658 ▲	$806,551,993 ▲	$347,657,432 ▲
Threats of Violence	$13,531,178 ▲	$4,972,099	N/A

OVERALL STATE STATISTICS

Complaints per State*					
Rank	*State*	*Complaints*	*Rank*	*State*	*Complaints*
1	California	77,271	30	Louisiana	4,890
2	Texas	47,305	31	Kentucky	4,641
3	Florida	41,061	32	District of Columbia	3,769
4	New York	26,948	33	Iowa	3,723
5	Ohio	17,864	34	Arkansas	3,220
6	Arizona	16,584	35	Mississippi	2,983
7	Pennsylvania	16,407	36	New Mexico	2,944
8	Illinois	15,783	37	Kansas	2,894
9	Michigan	14,784	38	Delaware	2,687
10	Washington	14,600	39	Puerto Rico	2,678
11	Georgia	13,917	40	West Virginia	2,365
12	Virginia	12,711	41	Alaska	2,338
13	North Carolina	12,282	42	Idaho	2,240
14	New Jersey	12,253	43	Nebraska	2,195
15	Colorado	11,475	44	Hawaii	1,954
16	Indiana	11,097	45	South Dakota	1,688
17	Massachusetts	9,915	46	New Hampshire	1,650
18	Nevada	9,893	47	Maine	1,626
19	South Carolina	9,736	48	Montana	1,571
20	Maryland	9,717	49	Rhode Island	1,425
21	Tennessee	8,484	50	Wyoming	828
22	Missouri	8,108	51	North Dakota	764
23	Wisconsin	7,683	52	Vermont	698
24	Minnesota	7,049	53	U.S. Minor Outlying Islands	145
25	Oregon	6,724	54	Virgin Islands, U.S.	126
26	Alabama	5,763	55	Guam	90
27	Connecticut	5,216	56	American Samoa	33
28	Utah	5,061	57	Northern Mariana Islands	16
29	Oklahoma	4,987			

*Note: This information is based on the total number of complaints from each state, American Territory, and the District of Columbia when the complainant provided state information. Please see Appendix B for more information regarding IC3 data.

OVERALL STATE STATISTICS *continued*

Losses by State*					
Rank	*State*	*Loss*	*Rank*	*State*	*Loss*
1	California	$2,159,454,513	30	Louisiana	$78,286,085
2	Texas	$1,021,547,286	31	Oklahoma	$66,967,060
3	Florida	$874,725,493	32	Iowa	$59,829,482
4	New York	$749,955,480	33	Hawaii	$51,722,052
5	New Jersey	$441,151,263	34	Idaho	$50,631,580
6	Pennsylvania	$360,334,651	35	Kentucky	$48,746,051
7	Illinois	$335,764,223	36	Arkansas	$46,585,087
8	Arizona	$324,352,644	37	District of Columbia	$46,142,350
9	Georgia	$301,001,997	38	Montana	$45,554,368
10	Washington	$288,691,091	39	New Mexico	$45,127,386
11	Virginia	$265,073,590	40	Nebraska	$40,581,244
12	Massachusetts	$235,890,173	41	South Dakota	$35,855,494
13	North Carolina	$234,972,238	42	Delaware	$35,376,770
14	Maryland	$221,520,527	43	Mississippi	$32,144,078
15	Michigan	$203,445,988	44	Alaska	$31,771,278
16	Nevada	$200,995,121	45	Rhode Island	$31,586,831
17	Ohio	$197,365,326	46	Puerto Rico	$30,102,231
18	Minnesota	$193,949,414	47	New Hampshire	$27,178,268
19	Colorado	$187,621,731	48	West Virginia	$21,445,942
20	Indiana	$162,259,036	49	Maine	$18,968,567
21	Tennessee	$161,195,036	50	Wyoming	$13,746,109
22	Oregon	$136,052,036	51	North Dakota	$13,532,443
23	Utah	$132,257,035	52	Vermont	$ 8,818,181
24	Missouri	$123,405,404	53	U.S. Minor Outlying Islands	$3,588,797
25	Connecticut	$120,767,349	54	Virgin Islands, U.S.	$2,637,004
26	South Carolina	$119,950,630	55	Guam	$747,876
27	Alabama	$96,479,649	56	American Samoa	$327,467
28	Kansas	$94,158,337	57	Northern Mariana Islands	$25,917
29	Wisconsin	$92,084,459			

*Note: This information is based on the total number of complaints from each state, American Territory, and the District of Columbia when the complainant provided state information. Please see Appendix B for more information regarding IC3 data.

OVERALL STATE STATISTICS *continued*

Count of Subjects per State*					
Rank	*State*	*Subjects*	*Rank*	*State*	*Subjects*
1	California	42,590	30	Kentucky	1,760
2	Texas	18,194	31	Mississippi	1,738
3	Florida	17,174	32	Nebraska	1,696
4	New York	14,824	33	Wisconsin	1,621
5	Georgia	6,083	34	Arkansas	1,587
6	Ohio	5,728	35	Utah	1,440
7	Illinois	5,550	36	New Mexico	1,035
8	Washington	5,523	37	Delaware	1,027
9	Pennsylvania	5,359	38	Kansas	989
10	Arizona	5,029	39	Iowa	915
11	North Carolina	4,973	40	West Virginia	736
12	Michigan	4,839	41	Idaho	694
13	New Jersey	4,633	42	South Dakota	615
14	Connecticut	4,297	43	Hawaii	602
15	Virginia	4,202	44	Montana	600
16	Colorado	4,178	45	Vermont	598
17	Maryland	3,598	46	Wyoming	573
18	Nevada	3,402	47	Rhode Island	525
19	Massachusetts	3,263	48	Alaska	487
20	Tennessee	3,127	49	New Hampshire	474
21	South Carolina	2,893	50	Maine	446
22	Indiana	2,624	51	Puerto Rico	326
23	Minnesota	2,549	52	North Dakota	303
24	Missouri	2,470	53	Virgin Islands, U.S.	60
25	Alabama	2,408	54	United States Minor Outlying Islands	58
26	Oregon	2,253	55	Guam	32
27	Louisiana	2,128	56	American Samoa	10
28	Oklahoma	2,066	57	Northern Mariana Islands	6
29	District of Columbia	1,952			

*Note: This information is based on the total number of complaints from each state, American Territory, and the District of Columbia when the complainant provided state information. Please see Appendix B for more information regarding IC3 data.

OVERALL STATE STATISTICS *continued*

Losses Attributed to Subjects per Destination State*					
Rank	*State*	*Loss*	*Rank*	*State*	*Loss*
1	California	$1,450,468,117	30	Delaware	$26,679,171
2	New York	$659,190,424	31	Oklahoma	$25,955,810
3	Florida	$460,557,456	32	Alabama	$24,130,582
4	Texas	$436,917,629	33	Iowa	$22,875,411
5	Washington	$197,573,721	34	Wisconsin	$21,885,467
6	New Jersey	$162,556,627	35	Kentucky	$18,985,386
7	Pennsylvania	$161,290,998	36	New Hampshire	$16,725,453
8	Illinois	$160,429,405	37	South Dakota	$16,664,530
9	Arizona	$143,931,864	38	Idaho	$16,259,172
10	Georgia	$138,867,559	39	New Mexico	$15,968,662
11	Utah	$136,063,240	40	Arkansas	$13,170,026
12	Colorado	$123,104,339	41	Montana	$12,196,983
13	Massachusetts	$115,059,569	42	West Virginia	$11,423,197
14	North Carolina	$100,992,438	43	Mississippi	$11,309,747
15	Minnesota	$76,391,448	44	Nebraska	$11,260,461
16	Louisiana	$76,222,392	45	Hawaii	$11,086,273
17	Maryland	$72,488,154	46	Kansas	$10,734,529
18	Nevada	$72,469,793	47	Rhode Island	$9,446,947
19	Virginia	$69,306,635	48	Maine	$7,468,102
20	District of Columbia	$65,746,127	49	Alaska	$6,534,122
21	Ohio	$64,966,735	50	Puerto Rico	$3,260,842
22	Michigan	$52,994,817	51	North Dakota	$2,714,457
23	Tennessee	$49,887,333	52	Vermont	$2,003,750
24	Indiana	$49,381,324	53	United States Minor Outlying Islands	$947,386
25	Missouri	$46,655,163	54	Northern Mariana Islands	$237,597
26	Connecticut	$40,616,316	55	Virgin Islands, U.S.	$123,269
27	Oregon	$38,230,223	56	Guam	$113,518
28	South Carolina	$31,866,254	57	American Samoa	$21,420
29	Wyoming	$30,627,210			

*Note: This information is based on the total number of complaints from each state, American Territory, and the District of Columbia when the complainant provided state information. Please see Appendix B for more information regarding IC3 data.

OVERALL STATE STATISTICS *continued*

Complaints per Capita*					*per 100,000 citizens*
Rank	*State*	*Subjects*	*Rank*	*State*	*Subjects*
1	District of Columbia	555.1	27	West Virginia	133.6
2	Alaska	318.8	28	New Jersey	131.9
3	Nevada	309.7	29	Missouri	130.9
4	Delaware	260.4	30	Rhode Island	130.0
5	Arizona	223.2	31	Wisconsin	130.0
6	California	198.3	32	Pennsylvania	126.6
7	Colorado	195.2	33	Georgia	126.2
8	Washington	186.9	34	Illinois	125.8
9	South Dakota	183.6	35	Oklahoma	123.0
10	Florida	181.6	36	Minnesota	122.8
11	South Carolina	181.2	37	Tennessee	119.0
12	Indiana	161.7	38	New Hampshire	117.7
13	Oregon	158.8	39	Maine	116.5
14	Maryland	157.2	40	Iowa	116.1
15	Texas	155.1	41	Idaho	114.0
16	Ohio	151.6	42	North Carolina	113.3
17	Utah	148.1	43	Alabama	112.8
18	Michigan	147.3	44	Nebraska	110.9
19	Virginia	145.8	45	Vermont	107.8
20	Connecticut	144.2	46	Louisiana	106.9
21	Wyoming	141.8	47	Arkansas	105.0
22	Massachusetts	141.6	48	Kentucky	102.5
23	New Mexico	139.2	49	Mississippi	101.5
24	Montana	138.7	50	Kansas	98.4
25	New York	137.7	51	North Dakota	97.5
26	Hawaii	136.2	52	Puerto Rico	83.5

*Note: This information is based on the estimated 2023 Census data and the total number of complaints from each state, the District of Columbia, and Puerto Rico when the complainant provided state information. Please see Appendix B for more information regarding IC3 data.

https://www.census.gov/data/tables/time-series/demo/popest/2020s-state-total.html#v2023

OVERALL STATE STATISTICS *continued*

Losses per Capita*					*per 100,000 citizens*
Rank	*State*	*Loss*	*Rank*	*State*	*Loss*
1	District of Columbia	$6,795,914	27	Illinois	$2,675,478
2	Nevada	$6,292,550	28	Idaho	$2,577,030
3	California	$5,542,009	29	Indiana	$2,364,534
4	New Jersey	$4,748,238	30	Wyoming	$2,353,556
5	Arizona	$4,364,657	31	Tennessee	$2,261,914
6	Alaska	$4,332,018	32	South Carolina	$2,232,240
7	Montana	$4,021,353	33	North Carolina	$2,168,543
8	South Dakota	$3,900,228	34	New Mexico	$2,134,317
9	Utah	$3,869,729	35	Nebraska	$2,051,237
10	Florida	$3,868,631	36	Michigan	$2,026,907
11	New York	$3,831,931	37	Missouri	$1,991,645
12	Washington	$3,695,066	38	New Hampshire	$1,938,461
13	Hawaii	$3,603,978	39	Alabama	$1,888,622
14	Maryland	$3,584,328	40	Iowa	$1,865,588
15	Delaware	$3,428,347	41	North Dakota	$1,726,240
16	Minnesota	$3,380,137	42	Louisiana	$1,711,639
17	Massachusetts	$3,369,186	43	Ohio	$1,674,584
18	Texas	$3,348,973	44	Oklahoma	$1,651,948
19	Connecticut	$3,338,719	45	Wisconsin	$1,557,861
20	Oregon	$3,213,809	46	Arkansas	$1,518,551
21	Kansas	$3,202,070	47	Puerto Rico	$1,479,384
22	Colorado	$3,192,143	48	Vermont	$1,361,957
23	Virginia	$3,041,335	49	Maine	$1,359,051
24	Rhode Island	$2,882,110	50	West Virginia	$1,211,587
25	Pennsylvania	$2,779,999	51	Mississippi	$1,093,451
26	Georgia	$2,729,130	52	Kentucky	$1,076,986

*Note: This information is based on the estimated 2023 Census data and the total number of complaints from each state, the District of Columbia, and Puerto Rico when the complainant provided state information. Please see Appendix B for more information regarding IC3 data.

https://www.census.gov/data/tables/time-series/demo/popest/2020s-state-total.html#v2023

APPENDIX A: DEFINITIONS

Advanced Fee: An individual pays money to someone in anticipation of receiving something of greater value in return, but instead, receives significantly less than expected or nothing.

Business Email Compromise (BEC): BEC is a scam targeting businesses or individuals working with suppliers and/or businesses regularly performing wire transfer payments. These sophisticated scams are carried out by fraudsters by compromising email accounts and other forms of communication such as phone numbers and virtual meeting applications, through social engineering or computer intrusion techniques to conduct unauthorized transfer of funds.

Botnet: A botnet is a group of two or more computers controlled and updated remotely for an illegal purchase such as a Distributed Denial of Service or Telephony Denial of Service attack or other nefarious activity.

Confidence/Romance: An individual believes they are in a relationship (family, friendly, or romantic) and are tricked into sending money, personal and financial information, or items of value to the perpetrator or to launder money or items to assist the perpetrator. This includes the Grandparent's Scheme and any scheme in which the perpetrator preys on the targeted individual's "heartstrings."

Credit Card Fraud/Check Fraud: Credit card fraud is a wide-ranging term for theft and fraud committed using a credit card or any similar payment mechanism (ACH, EFT, recurring charge, etc.) as a fraudulent source of funds in a transaction.

Crimes Against Children: Anything related to the exploitation of children, including child abuse.

Data Breach: A data breach in the cyber context is the use of a computer intrusion to acquire confidential or secured information. This does not include computer intrusions targeting personally owned computers, systems, devices, or personal accounts such as social media or financial accounts.

Employment: An individual believes they are legitimately employed and loses money, or launders money/items during the course of their employment.

Extortion: Unlawful extraction of money or property through intimidation or undue exercise of authority. It may include threats of physical harm, criminal prosecution, or public exposure.

Government Impersonation: A government official is impersonated in an attempt to collect money.

Harassment/Stalking: Repeated words, conduct, or action that serve no legitimate purpose and are directed at a specific person to annoy, alarm, or distress that person. Engaging in a course of conduct directed at a specific person that would cause a reasonable person to fear for his/her safety or the safety of others or suffer substantial emotional distress.

Identity Theft: Someone wrongfully obtains and uses personally identifiable information in some way that involves fraud or deception, typically for economic gain.

Investment: Deceptive practice that induces investors to make purchases based on false information. These scams usually offer those targeted large returns with minimal risk. (Retirement, 401K, Ponzi, Pyramid, etc.).

IPR/Copyright and Counterfeit: The illegal theft and use of others' ideas, inventions, and creative expressions – what's called intellectual property – everything from trade secrets and proprietary products and parts to movies, music, and software.

Lottery/Sweepstakes/Inheritance: An individual is contacted about winning a lottery or sweepstakes they never entered, or to collect on an inheritance from an unknown relative.

Malware: Software or code intended to damage, disable, or capable of copying itself onto a computer and/or computer systems to have a detrimental effect or destroy data.

Non-Payment/Non-Delivery: Goods or services are shipped, and payment is never rendered (non-payment). Payment is sent, and goods or services are never received, or are of lesser quality (non-delivery).

Overpayment: An individual is sent a payment/commission and is instructed to keep a portion of the payment and send the remainder to another individual or business.

Personal Data Breach: A leak/spill of personal data which is released from a secure location to an untrusted environment. Also, a security incident in which an individual's sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, or used by an unauthorized individual.

Phishing/Spoofing: The use of unsolicited email, text messages, and telephone calls purportedly from a legitimate company requesting personal, financial, and/or login credentials.

Ransomware: A type of malicious software designed to block access to a computer system until money is paid.

Real Estate: Loss of funds from a real estate investment or fraud involving rental or timeshare property.

SIM Swap: The use of unsophisticated social engineering techniques against mobile service providers to transfer a victim's phone service to a mobile device in the criminal's possession.

Tech Support: Subject posing as technical or customer support/service.

Threats of Violence: An expression of an intention to inflict pain, injury, self-harm, or death not in the context of extortion.

APPENDIX B: ADDITIONAL INFORMATION ABOUT IC3 DATA

- As appropriate, complaints are reviewed by IC3 analysts, who apply a crime type and adjust the total loss.
- Crime Types and losses can be variable and can evolve based upon investigative or analytical proceedings. Statistics are an assessment taken at a point in time, which can change.
- Complainant/Entity is identified as the individual filing a complaint.
- Some complainants may have filed more than once, creating a possible duplicate complaint.
- All location-based reports are generated from information entered when known/provided by the complainant.
- Losses reported in foreign currencies are converted to U.S. dollars when possible.
- Complaint counts represent the number of individual complaints received from each state and do not represent the number of individuals filing a complaint.
- Subject is identified as the individual perpetrating the scam as reported by the complainant.
- "Count by Subjects per state" is the number of subjects per state, as reported by complainants.
- "Losses Attributed to Subjects per Destination State" is the amount swindled by the subject, as reported by the complainant, per state.

APPENDIX C: PUBLIC SERVICE ANNOUCEMENTS PUBLISHED

Title	Date
Scammers Targeting Owners of Timeshares in Mexico	3/3/2023
Criminals Steal Cryptocurrency through Play-to-Earn Games	3/9/2023
The FBI Warns of a Spike in Cryptocurrency Investment Schemes	3/14/2023
Business Email Compromise Tactics Used to Facilitate the Acquisition of Commodities and Defrauding Vendors	3/24/2023
For-Profit Companies Charging Sextortion Victims for Assistance and Using Deceptive Tactics to Elicit Payments	4/7/2023
Criminals Pose as Chinese Authorities to Target US-based Chinese Community	4/10/2023
Multinational Non-Governmental Organizations Potentially Exploited in Aftermath of Earthquakes Affecting Turkey and Syria	4/28/2023
The FBI Warns of False Job Advertisements Linked to Labor Trafficking at Scam Compounds	5/22/2023
Malicious Actors Manipulating Photos and Videos to Create Explicit Content and Sextortion Schemes (ic3.gov)	7/5/2023
Business Email Compromise: The $50 Billion Scam	7/9/2023
Increase in Tech Support Scams Targeting Older Adults and Directing Victims to Send Cash through Shipping Companies	7/18/2023
Criminals Pose as Non-Fungible Token (NFT) Developers to Target Internet Users with an Interest in NFT Acquisition	8/4/2023
Increase in Companies Falsely Claiming an Ability to Recover Funds Lost in Cryptocurrency Investment Scams	8/11/2023
Cyber Criminals Targeting Victims through Mobile Beta-Testing Applications (ic3.gov)	8/14/2023
FBI Guidance for Cryptocurrency Scam Victims	8/24/2023
Violent Online Groups Extort Minors to Self-Harm and Produce Child Sexual Abuse Material	9/12/2023
"Phantom Hacker" Scams Target Senior Citizens and Result in Victims Losing their Life Savings	9/29/2023
Situation in Israel	10/10/2023
Cybercriminals are Targeting Plastic Surgery Offices and Patients	10/17/2023
Additional Guidance on the Democratic People's Republic of Korea Information Technology Workers	10/18/2023
Scammers Solicit Fake Humanitarian Donations	10/24/2023
Threats Associated with the Israel-HAMAS Conflict	10/26/2023
2023 Holiday Shopping Scams	11/15/2023
FBI Warns of Scammers Targeting Senior Citizens in Grandparent Scams and Demanding Funds by Wire, Mail, or Couriers	11/17/2023
Threat of Violence Likely Heightened Throughout Winter	12/12/2023

K-12 Report

CIS MS-ISAC Cybersecurity Assessment of the 2022–2023 School Year

November 2023

CIS Center for Internet Security®

MS-ISAC® Multi-State Information Sharing & Analysis Center®

Contents

Who is this report for?

This report offers K-12 leaders, including superintendents, principals, and administrative staff, as well as IT leaders and cybersecurity practitioners, valuable industry-specific insights to inform their decisions regarding cyber risk. The information in this report can also help IT and cybersecurity professionals responsible for their organization's cybersecurity maturity better prioritize cyber defense measures to keep up with evolving cyber threats targeting K-12 organizations.

Where was content sourced for this report?

The following information details first-hand reported data from the 2022-2023 school year, as submitted to the MS-ISAC from multiple sources, including more than 4,600 K-12 entities in the MS-ISAC. Sources include data collected from 402 respondents to the 2022 Nationwide Cybersecurity Review (NCSR), MS-ISAC member feedback, service, direct reporting data from the CIS Security Operations Center (SOC), and threat data and associated analysis by the CIS Cyber Threat Intelligence (CTI) Team.

Who We Are

The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation. CIS is a community-driven nonprofit, responsible for the globally-recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats. CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities.

The MS-ISAC is federally funded by CISA and a division of the Center for Internet Security (CIS). The MS-ISAC is autonomously guided by its Executive Committee and member organizations. The mission of the MS-ISAC is to improve the overall cybersecurity posture of over 16,000 U.S. State, Local, Tribal, and Territorial (SLTT) government organizations through coordination, collaboration, cooperation, and increased communication. The MS-ISAC offers members no-cost incident response and remediation support through our team of security experts and develop tactical, strategic, and operational intelligence, along with advisories that offer actionable information for improving organizational cyber maturity.

The Nationwide Cybersecurity Review (NCSR) is a no-cost, anonymous, annual self-assessment. All states (and agencies), local governments (and departments), tribal nations, and territorial governments are encouraged to participate. It is designed to measure gaps and capabilities of SLTT governments' cybersecurity programs and is based on the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF).

CIS is home to the MS-ISAC and the EI-ISAC.

The MS-ISAC is a trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial (SLTT) government entities.

The EI-ISAC supports the rapidly changing cybersecurity needs of U.S. SLTT election offices.

CISA focuses on the cybersecurity of all critical infrastructure within the United States (including election offices).

Executive Summary

K-12 leaders and IT and cyber professionals have faced significant challenges over the last several years. The complexities of shifting between in-person, virtual, and hybrid schooling have been met with an increasingly complicated and evolving cyber threat landscape where K-12 schools have become primary targets of cyber threat actors (CTAs). At the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), K-12 schools represent more than a quarter of our 16,000+ member organizations across the country.

If your school or district is not currently a member of the MS-ISAC, you're missing out on some powerful no-cost and low-cost tools and resources to assist your cybersecurity program. Learn more at www.cisecurity.org/ms-isac/.

The Center for Internet Security, Inc. (CIS®) collected first-hand data for the 2022-2023 school year through the Nationwide Cybersecurity Review (NCSR), feedback from MS-ISAC members, and data from the CIS Security Operations Center (CIS SOC). This data empowers K-12 leaders to make informed decisions regarding cyber risk and provides K-12 IT and cybersecurity professionals with a comprehensive understanding of the cyber threat landscape and practical guidance for improving cyber defenses. Key report highlights include:

Nationwide Cybersecurity Review (NCSR) Assessment: According to the assessment responses, the K-12 districts' leading concern is insufficient funding and inadequate cybersecurity resources.

Maturity Findings: K-12 schools are performing well in Identity Management and Access Control, Awareness and Training, and Maintenance; however, they report the lowest maturity in Protective Technologies, Information Protection Processes & Procedures, Supply Chain Risk Management, and Detection Processes.

Ransomware Findings: Ransomware continues to be one of the top concerns for K-12 organizations, so organizations should prepare and test for the efficacy of their incident response plans to limit the scope and impact before a full-blown attack.

Top 10 Malware: Qakbot, CoinMiner, and Tinba were the top three malware families affecting K-12 schools.

Top 5 K-12 Non-Malware Threats: The top two non-malware threats affecting K-12 entities were AsyncRAT and MageCart.

K-12 Web Security Trends: Malware still ranks as the most blocked threat in MDBR.

COSN EdTech Survey: Survey results revealed that cybersecurity was the number-one priority this year and budget constraints remain the number-one challenge facing EdTech Leaders.

K-12 Community Assessment

Now in its 20th year, the MS-ISAC supports more than 16,000 organizational members from among U.S. State, Local, Tribal, and Territorial (SLTT) governments. More than 4,600 of these members are K-12 schools and districts. K-12 has been the fastest-growing MS-ISAC member segment for the past four years. While the cyber threat against K-12 schools has increased significantly since 2020, these important organizations continue to face the challenges of limited technical staff and financial resources to enact cybersecurity measures.

Top Five Security Concerns

K-12 respondents to the 2022 NCSR reported their top five security concerns as follows:

Lack of sufficient funding	**81%** **of participants**
Increasing sophistication of threats	**59%** **of participants**
Lack of documented processes	**58%** **of participants**
Lack of a cybersecurity strategy	**47%** **of participants**
Inadequate availability of cybersecurity professionals	**41%** **of participants**

Data timeframe: July 1, 2022 – June 30, 2023

From the 2021 NCSR to the 2022 assessment, K-12 institutions consistently identified the same top five security concerns, with the leading concern being insufficient funding.

Staffing, Frameworks, Recovery Planning, and Reporting

K-12 School District Staffing

90% of K-12 school districts stated they have less than 5 employees with security-related duties.

K-12 School Districts and Security Framework Usage

68% of K-12 school districts stated they use a security framework, such as the CIS Critical Security Controls (CIS Controls) or the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). On average, K-12 school districts that use a security framework scored 36% higher on NCSR maturity scoring compared to those not using a framework.

Response and Recovery Planning

23% responded "Not Performed" for the assessment question specific to having response plans and recovery plans in place. K-12 NCSR participants that are performing this activity, and/or have documented policies/procedures applicable to a response plan and a recovery plan, displayed 94% higher overall average NCSR maturity scoring than K-12 NCSR participants that are not performing these activities.

Cyber Reporting to Decision Makers

59% stated they provide periodic (at least annual) information risk, control, and security reporting to top-level decision-makers. Those who provided periodic cyber reporting to decision-makers displayed 52% higher overall average NCSR maturity scoring than those organizations that did not perform this activity.

Maturity Findings of the K-12 Sector

The Nationwide Cybersecurity Review (NCSR) is a voluntary, annual self-assessment designed to help organizations establish a baseline score of their cybersecurity maturity, on a scale of 1 through 7, according to the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF). Numerous state and federal grant programs require completion of the NCSR to qualify for funding. The 2022 NCSR results highlighted numerous trends in K-12 cybersecurity maturity.

Overall

2022 saw the highest participation rate for K-12 organizations in the NCSR's 11-year history, with 402 members completing the assessment. The overall average maturity score of K-12 NCSR participants was 3.25, compared to last year's score of 3.55. The 2022 score, although slightly lower than the 2021 score and below local sectors like public utilities, health services, and election offices, still stands at a satisfactory level of "3."

High Maturity Categories

Areas where K-12 schools are generally performing well include:

Identity Management and Access Control	Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.
Awareness and Training	Organizations' personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.
Maintenance	Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.

In addition to Identity Management and Access Control and Awareness and Training retaining their top two positions from the 2021 NCSR, K-12 schools are also demonstrating improved performance in the Maintenance category when compared to last year's assessment, where Business Environment ranked as the third highest maturity category.

Low Maturity Categories

Areas where K-12 schools are generally performing poorly include:

	ASSOCIATED BEST PRACTICES TO IMPLEMENT	
NIST CSF Category	**CIS Critical Security Control**	**Recommended Actions**
Protective Technologies	**CIS Control 3:** Data Protection	• Establish and Maintain a Data Classification Scheme • Document Data Flows • Encrypt Data on Removable Media
	CIS Control 8: Audit Log Management	• Collect Audit Logs
	CIS Control 10: Malware Defenses	• Disable Autorun and Autoplay for Removable Media
Information Protection Processes and Procedures	**CIS Control 7:** Continuous Vulnerability Management	• Perform Automated Vulnerability Scans of Externally Exposed Enterprise Assets
Supply Chain Risk Management	**CIS Control 11:** Data Recovery	• Test Data Recovery
	CIS Control 15: Service Provider Management	• Monitor Service Providers
Detection Processes	**CIS Control 17:** Incident Response Management	• Designate Personnel to Manage Incident Handling • Establish and Maintain an Incident Response Process • Conduct Routine Incident Response Exercises • Conduct Post-Incident Reviews

These categories reflect the three NIST categories with the lowest maturity as reported by K-12 schools in the 2022 NCSR. These categories have been mapped to the corresponding CIS Critical Security Controls® (not presented in order of importance). While Protective Technologies and Supply Chain Risk Management remain as areas with low maturity scores for K-12 schools, they now also exhibit low maturity scores in Information Protection Processes & Procedures and Detection Processes, which were not reported as low-performing categories in the 2021 assessment. To ensure that you're meeting the minimum standard of security maturity, CIS recommends K-12 schools start with Implementation Group 1 (IG1) of the CIS Controls.

Ransomware Findings

Ransomware continues to be one of the top concerns for K-12 organizations, and it is essential for organizations to prepare and test for the efficacy of their incident response plans to limit the scope and impact before a full-blown attack.

What Happened?

During the 2022-2023 school year, a K-12 district was impacted by ransomware. They notified the MS-ISAC of the incident after receiving mixed results with the commercial vendor who initially was primary on incident response.

How Did the MS-ISAC Respond?

The MS-ISAC Security Operations Center (SOC) supporting MS-ISAC members took the initial incident report, collected incident details, and connected the member to the MS-ISAC Cyber Incident Response Team (CIRT). After scoping the incident on an initial incident response call, CIRT provided guidance and tools to the member to collect forensic artifacts and logs. This included artifacts and logs from the affected domain and configuration servers, which helped to better assess the threat actor's actions and establish indicators of compromise (IOCs). As part of interdepartmental MS-ISAC coordination, the MS-ISAC Cyber Threat Intelligence (CTI) team provided additional intelligence on the threat actor to assist CIRT's efforts. CIRT provided scripts to the impacted school district to determine where identified IOCs were present in their IT environment. Additionally, CIRT provided guidance to assist with the recovery effort and identified the threat actor's ransomware binary that was used to encrypt files. All this work led to establishing a timeline of events going from initial access to data exfiltration and encryption.

What Was the Impact?

The MS-ISAC response by SOC, CIRT, and CTI teams provided the affected school district with timely assistance. As a result, the school district better understood how to identify and investigate the threat activity. The district indicated that the MS-ISAC response was instrumental in understanding the incident timeline, developing IOCs, and obtaining necessary guidance to help restore the network. They were especially appreciative for the "above and beyond" efforts that the CIRT provided to help restore access to school enterprise systems during a busy school year.

Here are some actions you can take today to reduce the risk and impact from ransomware:

Prioritize and remediate known exploited vulnerabilities

For the benefit of the cybersecurity community and network defenders—and to help every organization better manage vulnerabilities and keep pace with threat activity—the Cybersecurity and Infrastructure Security Agency (CISA) maintains the authoritative source of vulnerabilities that have been exploited in the wild: the **Known Exploited Vulnerability (KEV) catalog**.

The KEV catalog sends a clear message to all organizations to prioritize remediation efforts on the subset of vulnerabilities that are causing immediate harm based on adversary activity. Organizations should use the KEV catalog as an input to their vulnerability management prioritization framework.

Train users to recognize and report phishing attempts

Teach employees to keep their guard up on all communications platforms, including social media, and flag suspicious correspondence for security review.

Educate employees on what to do when they receive a phishing email—regardless of whether they fell for it.

Enable and enforce multi-factor authentication

Require phishing-resistant multi-factor authentication (MFA) for all services to the extent possible, particularly for webmail, virtual private networks (VPNs), and accounts that access critical systems.

Incident Response

We recommend that K-12 schools have an incident response (IR) plan in place when a cyber risk is detected. The primary goal of IR is to identify threats on the enterprise, respond to them before they can spread, and remediate them before they can cause harm. One crucial aspect of incident response planning is making sure your plans can be efficiently executed when an incident occurs. Partners in need of assistance with incident planning can join the Business Resiliency Working Group and later become members of our Incident Response Planning and Operations Workbench community.

To help develop an IR plan, K-12 organizations can use tabletop exercises to consider different risk scenarios, prepare for potential cyber threats, and identify tactical strategies for securing their systems. Tabletop exercises are designed to help organizations consider different risk scenarios and prepare for potential cyber threats. All the exercises can be completed in as little as 15 minutes, making them a convenient tool for putting your team in the cybersecurity mindset. In addition, each scenario will list the processes being tested, threat actors identified, as well as the impacted assets.

The incident response process consists of four steps: Plan, Detect, Respond, and Update.

Plan

Develop documentation for all procedures necessary to handle an incident.

Detect

Monitor enterprise assets and analyze intelligence to understand if an incident has occurred.

Respond

Activate the incident response plan to deal with an incident.

Update

Understand which portions of the incident response plan have been effective and update the plan accordingly.

K-12 organizations can report incidents by calling the CIS SOC at 866-878-4722 or emailing soc@cisecurity.org.

Additionally, CIS and CoSN have developed the K-12 Cybersecurity Incident Response Steps that outline the actions K-12 organizations can take before and during a cybersecurity incident.

CIS Center for Internet Security®

CoSN LEADING EDUCATION INNOVATION

Who you should call when a cyber incident strikes

Law Enforcement

It's important to inform appropriate law enforcement authorities at the outset of a cyber incident.

Cyber Insurance

Cyber insurance companies may have stipulations guiding your initial actions in the event of a cyber incident.

CIS SOC

The CIS Security Operations Center (SOC) regularly supports public sector organizations during cyber incidents, providing initial recommendations, analyzing indicators of compromise (IOCs), and assisting with mitigation.

Industry-specific Contacts

Organizations in certain industries may have specific notification requirements when experiencing a cyber incident.

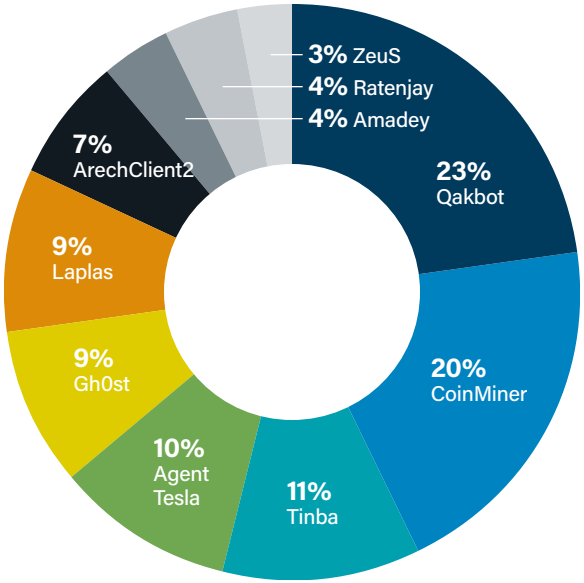
Internal Contacts

Following your incident response plan should involve notifying appropriate leaders and individuals in your organization of a cyber incident.

Top 10 Malware Affecting K-12 Schools

CIS, through the MS-ISAC, maintains the largest database for security threats against U.S. SLTT governments, including K-12 schools. This SLTT-specific threat database is informed by Albert IDS telemetry.

From August 2022 through May 2023, Qakbot and CoinMiner were the top two malware affecting K-12 entities, making up 43% of the Top 10 Malware. This contrasts with the prior year's assessment when Shlayer, a type of malware that targets Apple macOS, posed the most significant threat to K-12 entities.



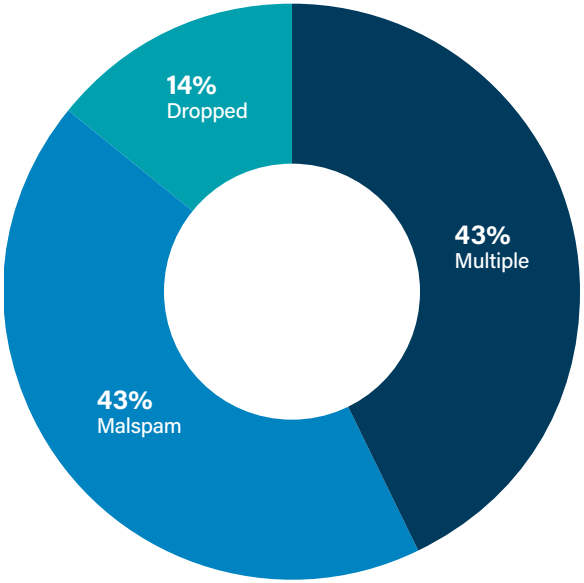
QakBot is a versatile banking Trojan with a wide range of capabilities, including enumeration (using commands like net, whoami, nslookup, netstat, ipconfig, etc.), lateral movement through SMB, keylogging to steal user credentials, network traffic monitoring, and the ability to deploy additional malware. Specifically, it targets online banking websites using a Man-in-the-Middle (MitM) technique to intercept authentication tokens during active banking sessions. QakBot can also load various modules, including credential and cookie harvesters, a Virtual Network Computing (VNC) module, Cobalt Strike, and an email collection module. Furthermore, it can lead to other malware infections, such as ransomware. After its operators are done with an infected host or network, QakBot uses Cobalt Strike modules to sell or grant access to other cyber threat actor (CTA) groups. It spreads primarily through malspam, often involving thread hijacking.

CoinMiner, a cryptocurrency miner family, typically employs Windows Management Instrumentation (WMI) for network propagation. It frequently relies on WMI Standard Event Consumer scripting for persistence, though its capabilities may vary due to multiple variants. CoinMiner is usually distributed through malspam or as a payload dropped by other malware.

Tinba, also known as Tiny Banker, is a banking Trojan distinguished by its compact file size. It uses web injections to capture victim information from login pages and web forms and is primarily disseminated through exploit kits.

From August 2022 through May 2023, Qakbot and CoinMiner were the top two malware affecting K-12 entities, making up 43% of the Top 10 Malware.

How Cyber Attackers Gain Access



CIS tracks potential initial infection vectors for the Top 10 Malware each quarter based on open-source reporting, as depicted in the graph below. We currently track four initial infection vectors: Dropped, Malvertisement, Malspam, and Network. Some malware uses different vectors in different contexts and are tracked as Multiple.

43%

Multiple

Malware that currently favors at least two vectors, such as Dropped and Malspam.

43%

Malspam

Unsolicited emails that either direct users to malicious websites or trick users into downloading or opening malware. Agent Tesla, Kovter, and NanoCore are using this technique.

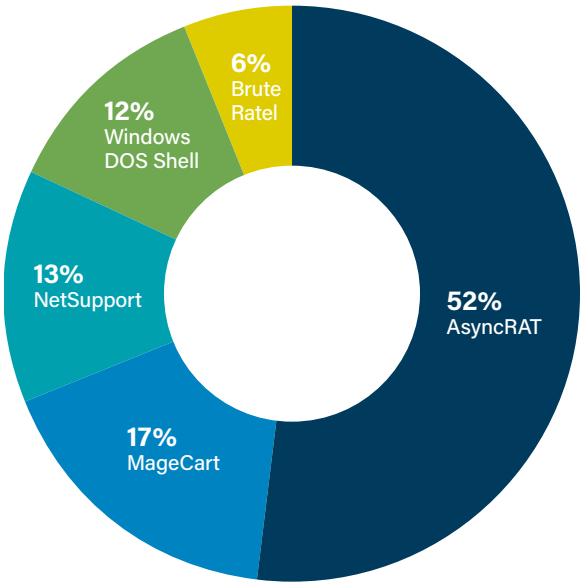
14%

Dropped

Data from Albert Network Monitoring and Management revealed that, from August 2022 to May 2023, Multiple, Malspam, and Dropped remained prominent initial infection vectors. In contrast, Malvertisement dropped out of the top 10, likely due to Shlayer being the only malware using this technique, and Shlayer is no longer a significant threat to K-12 schools during this period.

Top 5 K-12 Non-Malware Threats

CTAs are increasingly leveraging legitimate remote monitoring and management tools to access and control victims' machines. By expanding their use of legitimate tools, CTAs are more effective at making their presence on a network appear legitimate, effectively hiding their activity among all the other legitimate activities and processes.



From August 2022 through May 2023, exploitation activity—the top two non-malware threats affecting K-12 entities were AsyncRAT and MageCart, making up 69% of the Top 5 Non-Malware threats observed by K-12 entities over that time. Interestingly, the Top 5 Non-Malware Threats in last year's MS-ISAC K-12 Cybersecurity Report have been supplanted this year by an entirely new set of threats. Changes in the Top 5 Non-Malware Threats from year to year occur for many reasons, most commonly due to the changing threat landscape, as well as CTAs continuing to evolve their tactics, techniques, and procedures (TTPs), abandoning TTPs that are no longer effective and employing TTPs that have a greater probability of achieving their goals.

AsyncRAT is an open-source Windows remote administration tool used for remote monitoring and control of computers via a secure encrypted connection. It is frequently misused with features like screen recording, keylogging, and remote desktop control, typically delivered through phishing, malvertising, and exploit kits.

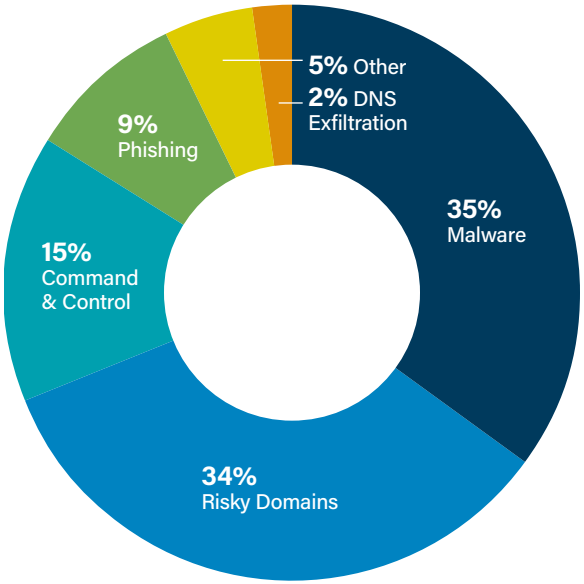
MageCart is a credit card skimming script that steals payment data from vulnerable website forms. Traffic to this domain suggests potential compromise of sensitive financial data on the affected host.

NetSupport is a remote access tool originally designed for providing technical support or computer assistance but is often exploited for malicious purposes, thanks to its remote desktop control capabilities and other features.

Three of the Top 5 Non-Malware Threats are legitimate tools, making up 72% of Top 5 Non-Malware Threat activity. AsyncRAT and NetSupport were the first and third respectively in this year's Top 5 Non-Malware Threats, making up 65% of the Top 5 non-malware activity. Both are legitimate remote access tools used for remote technical support or computer assistance. The third legitimate tool in the Top 5 Non-Malware is Brue Ratel, a tool used by security analysts to conduct penetration testing.

K-12 Web Security Trends

The Malicious Domain Blocking and Reporting (MDBR) service is a secure recursive DNS solution offered at no cost to K-12 schools. MDBR prevents IT systems from connecting to harmful web domains, helping limit infections related to known malware, ransomware, phishing, and other cyber threats.



Between August 2022 and May 2023, malware still ranked as the most blocked activity in MDBR, but there is a 25% decrease in K-12 schools reporting it as a trend compared to the 2022 K-12 Report.

CoSN EdTech Survey

CIS is proud to partner with the Consortium for School Networking (CoSN). CoSN provides thought leadership resources, community, best practices, and advocacy tools to help leaders succeed in digital transformation. CoSN currently represents more than 13 million students. Each year, CoSN conducts a survey to provide a national perspective on the EdTech landscape, the challenges EdTech Leaders face, and the successes they've had.

For a decade, CoSN has been asking EdTech Leaders about their top priorities. Although the number of options provided in the survey has increased from 16 to 26, comparisons provide insight into just how much has changed over the years.

What has not changed in 10 years though is the struggle with insufficient resources. Budget constraints remain the number-one challenge facing EdTech Leaders. Although budgets have increased over the years, so have the IT areas that budgets must fund.

Pertinent to this report, the additional findings outlined below provide a window into the state of K-12 cybersecurity and how K-12 organizations are mitigating risks within the limitations of overly-constrained budgets:

Inadequate Funding

Inadequate funding is glaringly apparent for the 12% of districts reporting zero allocation in their district's IT budget for sustaining cybersecurity defense.

Since 2018, survey respondents have consistently identified cybersecurity as their number-one priority.

Cybersecurity Insurance

Year-Over-Year Comparison of Cyber Insurance Policy Purchases

POLICY PURCHASED	2023	2022
Yes, separate	**31%**	24%
Yes, umbrella	**43%**	38%
No	**11%**	19%
Planning	**3%**	3%
Not sure	**11%**	16%

Cybersecurity insurance is purchased by 89% of all districts, an increase from 81% the prior year. Umbrella policies are the most common type, which account for 43%. The remaining balance of districts (31%) purchase cyber insurance as a separate policy. Districts that do not purchase insurance account for 11%, down from 19% in 2022. The percentage of EdTech Leaders who are not sure if their district has a policy is also down year over year, down to 11% from the previous 16%.

This is an encouraging sign, as it suggests more EdTech Leaders are part of the cybersecurity insurance discussion in their districts. Increasingly, insurance companies have prerequisites for purchase and requirements for payout. EdTech Leaders need to know the details to ensure the district can comply.

Top 5 Recommendations for K-12 Organizations

1

Join the MS-ISAC to gain a valuable partner in your cyber defense

By joining the MS-ISAC K-12 Working Group, you can establish connections with similar organizations and contribute to enhancing the collective cybersecurity stance of the community. You can also engage in networking and collaborative discussions with fellow cybersecurity experts within the CIS WorkBench Community, where you can share and learn about best practices for securing the technologies you rely on.

2

Complete the NCSR to gauge your cyber maturity

Haven't completely the NCSR yet? Request information about the abbreviated Foundational Assessment at foundationalassessment@cisecurity.org. The 32-question Foundational Assessment is for organizations looking to assess their cybersecurity programs but have not yet taken the more comprehensive NCSR.

3

Complete Implementation Group 1 (IG1) of the CIS Critical Security Controls

Protect your organization with globally-recognized cybersecurity best practices by claiming your no-cost CIS SecureSuite Membership to chart and guide your path toward IG1 implementation, which has proven to be between 77% and 86% effective at defending against common cyber attacks.

4

Sign up for the MS-ISAC Indicator Sharing Program

Receive near real-time cyber threat intelligence you can act on.

5

Implement an intrusion detection system (IDS) and endpoint detection and response (EDR)

Learn how to protect your IT environment with Albert Network Monitoring and Management and Endpoint Security Services (ESS) solutions offered by CIS to see if they are right for your organization.

Services Available to MS-ISAC Members

MS-ISAC membership is available at no-cost to all U.S. State, Local, Tribal, and Territorial (SLTT) government organizations. Members benefit from numerous no- and low-cost services and resources to help build and maintain effective cybersecurity programs.

CYBERSECURITY SERVICES	DESCRIPTION	NO COST	COST EFFECTIVE
Cyber Threat Intelligence			
Cyber Alerts and Advisories	Brief, timely emails containing information on specific cyber incidents/threats and vulnerabilities in software and hardware	✓	
Quarterly Threat Reports	Analysis of SLTT-focused cyber threat intelligence trends and threat forecasting	✓	
Regular IOCs	Weekly, monthly reports on malicious IPs/domains	✓	
White Papers	Technical papers providing relevant information on cyber threat topics	✓	
Cyber Threat Briefings	Informative sessions on the cyber threat landscape to SLTTs	✓	
Real-time Intelligence Feeds	Easy-to-implement real-time cyber threat intelligence indicator feeds derived from more than 200 sources and specific to SLTTs	✓	
Cybersecurity Services			
24x7x365 Security Operations Center (SOC)	Full-time cyber defense partner to member organizations that monitors, analyzes, and responds to cyber incidents affecting members	✓	
Malicious Domain Blocking & Reporting (MDBR)	Web security service that proactively blocks network traffic to known harmful web domains, protecting IT systems against cyber threats	✓	
Endpoint Security Services (ESS)	Device-level protection and response for active defense against both known (signature-based) and unknown (behavioral-based) malicious activity		✓
Albert Network Monitoring and Management	Cost-effective network Intrusion Detection System (IDS) tailored to SLTT governments' threat profile and security needs		✓
Managed Security Services (MSS)	Cost-effective log and security event monitoring of devices like IDS/IPS, firewalls, switches and routers, services, endpoints, and web proxies		✓
Penetration Testing	Services that simulate real-world cyber attacks on network and web applications and enable organizations to safely identify exploitable vulnerabilities		✓

Services Available to MS-ISAC Members (continued)

CYBERSECURITY SERVICES	DESCRIPTION	NO COST	COST EFFECTIVE
Security Best Practices			
CIS SecureSuite Membership	Comprehensive set of cybersecurity resources and tools to implement the CIS Critical Security Controls (CIS Controls) and CIS Benchmarks	✓	
Other Member Services and Resources			
MS-ISAC Webinars	Monthly member calls and webinars on topics of interest to the SLTT community	✓	
MS-ISAC Working Groups	Voluntary committees focused on collaboration among SLTT organizations to help drive MS-ISAC initiatives and member enrichment and growth	✓	
Nationwide Cybersecurity Review (NCSR)	Anonymous, annual self-assessment designed to evaluate cybersecurity maturity and set a baseline for organizational improvement	✓	
CIS CyberMarket	A collaborative purchasing program available to SLTTs that leverages collective purchasing power of our 16,000+ member organizations to provide low-cost security solutions from industry-leading cybersecurity providers		✓

About CIS

The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation. We are a community-driven nonprofit, responsible for the CIS Critical Security Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats. Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud. CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the rapidly changing cybersecurity needs of U.S. election offices. To learn more, visit www.CISecurity.org.

About the MS-ISAC

The Multi-State Information Sharing and Analysis Center® (MS-ISAC®) has been designated by the Cybersecurity & Infrastructure Security Agency (CISA) as the key resource for cyber threat prevention, protection, response, and recovery for all U.S. State, Local, Tribal, and Territorial (SLTT) governments. The mission of the MS-ISAC is to improve the overall cybersecurity posture of the nation's SLTT governments through coordination, collaboration, cooperation, and increased communication. The MS-ISAC is a division of the Center for Internet Security® (CIS®), a 501(c)(3) nonprofit. Visit www.cisecurity.org/ms-isac/ or email info@msisac.org for more information.

About CoSN

CoSN is the premier professional association for K-12 EdTech leaders, their teams, and other school district leaders. CoSN provides thought leadership resources, community, best practices, and advocacy tools to help leaders succeed at digital transformation. CoSN represents over 13 million students and continues to grow as a powerful and influential voice in K-12 education.

CoSN also provides opportunities for companies that support the K-12 EdTech community to participate as corporate members.

Acknowledgements

We extend our sincere gratitude to the dedicated teams at CIS who collectively contributed to the creation of this report. Their collaborative efforts spanned a wide range of critical tasks, from data collection and analysis to conducting polls and surveys, compiling data, writing, reviewing, designing, and much more.

CIS Cyber Threat Intelligence Team: The Cyber Threat Intelligence Team provided essential insights and analysis, enhancing the report's depth and accuracy.

CIS Cyber Incident Response Team: The Cyber Incident Response Team's expertise in incident handling and response contributed to the report's understanding of emerging threats and vulnerabilities.

CIS Security Operations Center Team: The Security Operations Center Team's continuous vigilance and monitoring efforts supported the report's emphasis on proactive threat mitigation.

CIS Nationwide Cybersecurity Review Team: The Nationwide Cybersecurity Review Team's data collection and analysis efforts formed the foundation of this report, enabling us to present comprehensive findings.

CIS Stakeholder Engagement Operations Team: The Stakeholder Engagement Operations Team ensured that the report's insights would be disseminated effectively to stakeholders and partners.

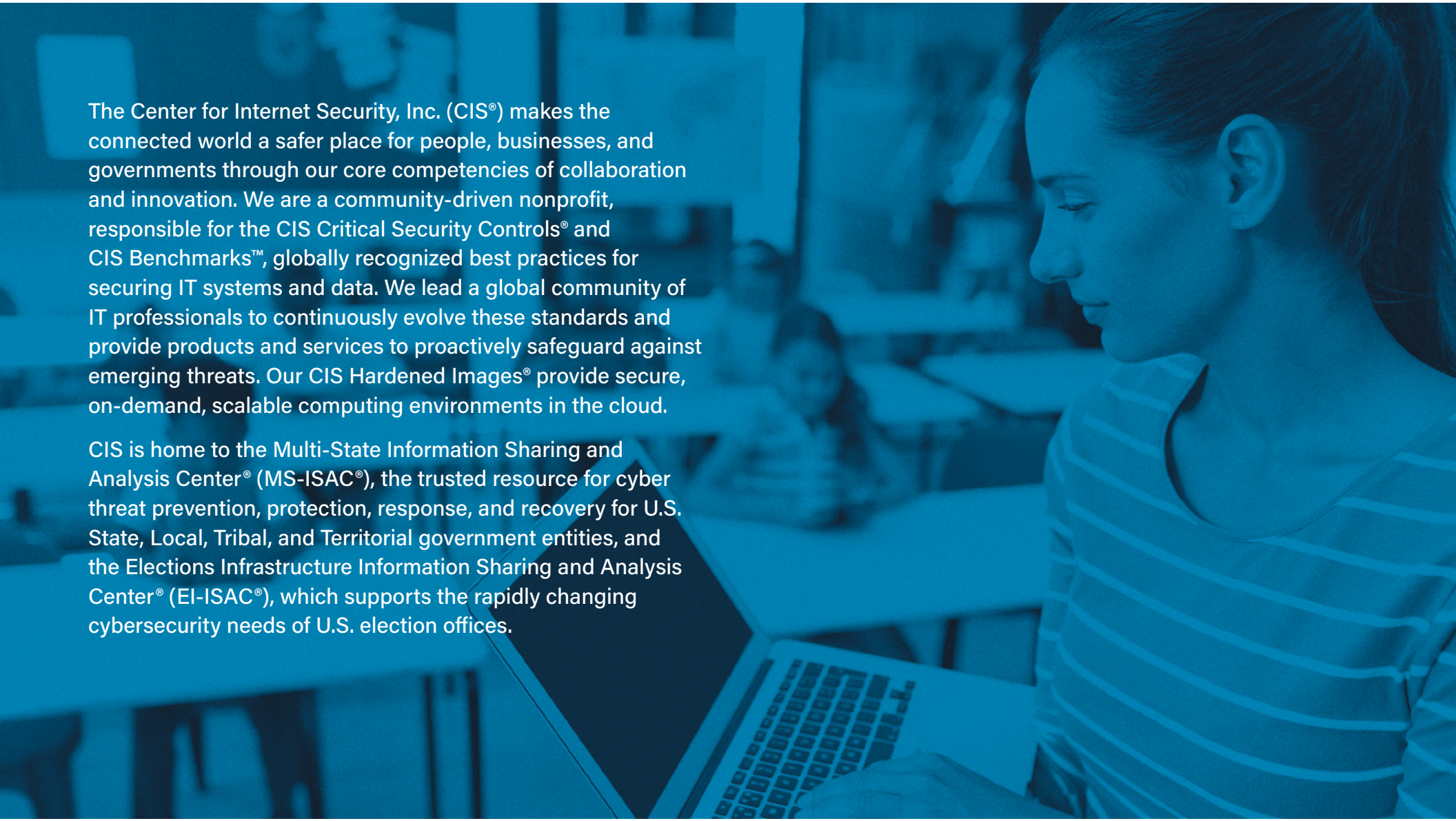
CIS Marketing and Communications Team: The Marketing and Communications Team played a pivotal role in crafting and conveying the message of this report, ensuring its clarity and reach.

We extend our sincere thanks to everyone involved in this project for their dedication, expertise, and unwavering support. The value your commitment brings to helping K-12 organizations increase their cyber maturity cannot be understated. Thank you!

Special Thanks

We'd like to thank our K-12 MS-ISAC members for their strong collaboration and hard work to improve cybersecurity across this vital community. Special thanks to the following individuals who went above and beyond to support this K-12 report: Scott Fosseen, John Wargo, Terry Loftus, Brad Hagg, and Bhargav Vyas.

We'd also like to extend our gratitude to Consortium for School Networking (CoSN) for their commitment to empowering K-12 leaders to succeed in the digital transformation through resources and advocacy tools. Special thanks to the CoSN and the CoSN Cybersecurity Advisory Committee for their outstanding support for, and contribution to, this report.



The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation. We are a community-driven nonprofit, responsible for the CIS Critical Security Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats. Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud.

CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the rapidly changing cybersecurity needs of U.S. election offices.

CIS Center for Internet Security®

MS-ISAC®
Multi-State Information Sharing & Analysis Center®

cisecurity.org
info@cisecurity.org
518-266-3460
Center for Internet Security
@CISecurity
TheCISecurity
cisecurity

THE STATE OF K-12 CYBERSECURITY: YEAR IN REVIEW

2022 Annual Report

K12 Security Information Exchange

K12 SIX

The *State of K-12 Cybersecurity: Year in Review* report is a product of the K12 Security Information Exchange (K12 SIX) based on data from the K-12 Cyber Incident Map, the definitive source of information about publicly disclosed cyber incidents affecting U.S. public schools and education agencies.

ABOUT THE K12 SECURITY INFORMATION EXCHANGE

The K12 Security Information Exchange (K12 SIX) is a national non-profit membership organization dedicated solely to helping protect K-12 schools—public and private—from emerging cybersecurity threats, such as ransomware and phishing attacks. It was launched in late 2020 as an affiliate of the Global Resilience Federation in response to the growing cybersecurity challenges facing schools nationwide, and in recognition of the unique challenges and context of K-12 operations.

Benefits of K12 SIX membership include:

- Engagement in a private, nationwide community of K-12 information security professionals via a secure communications platform
- Access to a cyberthreat information sharing portal and mobile app with actionable alerts, reports, and best practices
- Enrollment in the K12 SIX emergency notification system (via phone, email, and SMS) for issues that require immediate action
- Weekly virtual CISO open office hours and access to dedicated K12 SIX security analysts
- Weekly newsletters providing situational awareness tailored specifically to the K-12 community
- Semi-monthly and ad hoc member meetings to share information about—and coordinate joint actions in response to—incidents of significant impact, scale, and sensitivity
- Leadership, staff development and training opportunities, through participation in K12 SIX events, committees, and advisory groups

K12 SIX also works in partnership with other information sharing communities (ISACs and ISAOs), federal agencies, national and state education associations, and serves the broader K-12 sector through professional development, awareness-building, and advocacy. For more information, including on how school districts can participate, please visit https://www.k12six.org

---

TLP WHITE

Suggested Citation:

> Levin, Douglas A. (2022). "The State of K-12 Cybersecurity: Year in Review – 2022 Annual Report." K12 Security Information Exchange (K12 SIX). Available online at: https://www.k12six.org/the-report

ACKNOWLEDGEMENTS

Since the K-12 Cyber Incident Map first launched it has benefited from many individual and corporate supporters who have contributed financial and intellectual resources to its maintenance and ongoing development. This year's report was strengthened via collaborations with: Dissent Doe, the pseudonym of a privacy advocate and activist who blogs about privacy issues and data security breaches on PogoWasRight.org and DataBreaches.net; investigative reporters, including Kevin Collier (NBC News), Tanya Eiserer (WFAA Dallas), Grace Ferguson (Daily Dot), Dana Kozlov (CBS 2 Chicago), Brian New (CBS 11 Dallas Fort-Worth), Scott Travis (Sun Sentinel), and Julie Watts (CBS 13 Sacramento); and, Staci Elliott, Eric Lankford, Patrick McGlone, Cassandra Orsi, and Arshad Somani of K12 SIX.

2022 ANNUAL REPORT SPONSORS

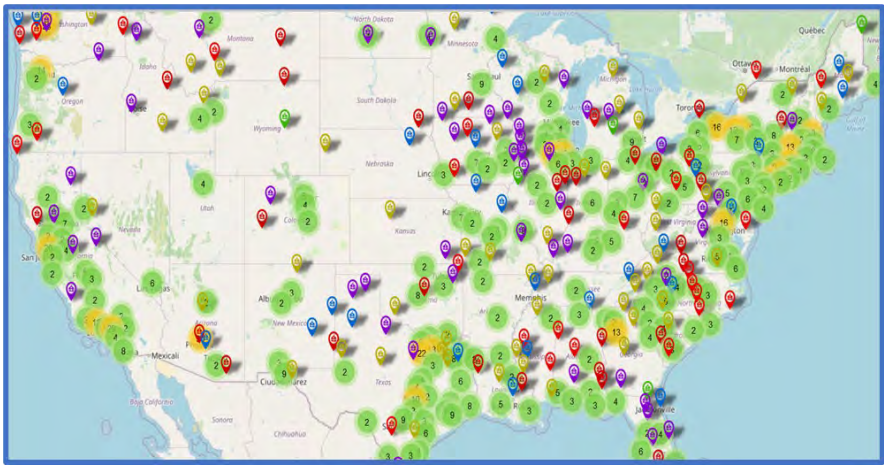
INTRODUCTION

School districts and their vendors regularly fall victim to cybersecurity threats, placing millions of students and teachers directly in harm's way.

If the response to the COVID pandemic has underscored anything, it is that the resiliency of the U.S. public education system is integral to the national economy and the well-being of communities—whether rural, suburban, or urban—across the nation. Serving over 50 million students in over 100,000 schools nationwide, the U.S. public education sector is an enormous—albeit highly decentralized—enterprise.[1]

While many outside the public education sector have been slow to recognize it, school districts (like other local government agencies) are amid a digital transformation of their operations—digitizing paper-based processes and adopting 'smart' technologies for core services including facilities management, transportation, HR/staffing, business services, and teaching and learning. While the adoption of technology provides benefits, it also introduces new risks—both to the resilience of school district operations as well as to the safety of school community members, including students and teachers.

This report is the fourth in an annual series[2] designed to shed light on cybersecurity incident trends in the U.S. K-12 public education sector, based on a data source that the U.S. Government Accountability Office (GAO) found to be the "most complete resource that tracks K-12 cybersecurity incidents, including student data breaches."[3] Published by the non-profit K12 Security Information Exchange (K12 SIX), it remains the first and only vendor-agnostic, independent research effort dedicated solely to cataloging and analyzing cybersecurity incidents affecting U.S. public K-12 school districts.



The K-12 Cyber Incident Map, a visualization of publicly disclosed school cyber incidents from 2016 to present. Available online at https://k12six.org/map

By focusing on publicly-disclosed incidents experienced by school districts and other public education agencies, this report provides unique insights into how K-12 cyber risk management practices are exploited and suggests how they may best be remedied. Nonetheless, an exclusive focus on publicly-

disclosed incidents also dramatically understates the scope of the issues facing K-12 schools, especially when disclosure requirements are weak and routinely circumvented. The true picture is surely bleaker; anecdotal evidence suggests perhaps 10 to 20 times more K-12 cyber incidents go undisclosed every year.

In the following sections, this report presents findings from detailed analyses of cyber incidents experienced by school districts, as well as the characteristics of those districts. It concludes with recommendations to address the growing challenge of cybersecurity risk management in the K-12 sector writ large. An appendix offers information on the data and methods relied on for this report.

"IT'S JUST THAT FEELING OF HELPLESSNESS, OF CONFUSION AS TO WHY SOMEBODY WOULD DO SOMETHING LIKE THIS BECAUSE AT THE END OF THE DAY, IT'S TAKING AWAY FROM OUR KIDS. AND TO ME THAT'S JUST A DISGUSTING WAY TO TRY TO, TO GET MONEY," SUPERINTENDENT CHANNELL SEGURA [TRUTH OR CONSEQUENCES MUNICIPAL SCHOOL DISTRICT] SAID.

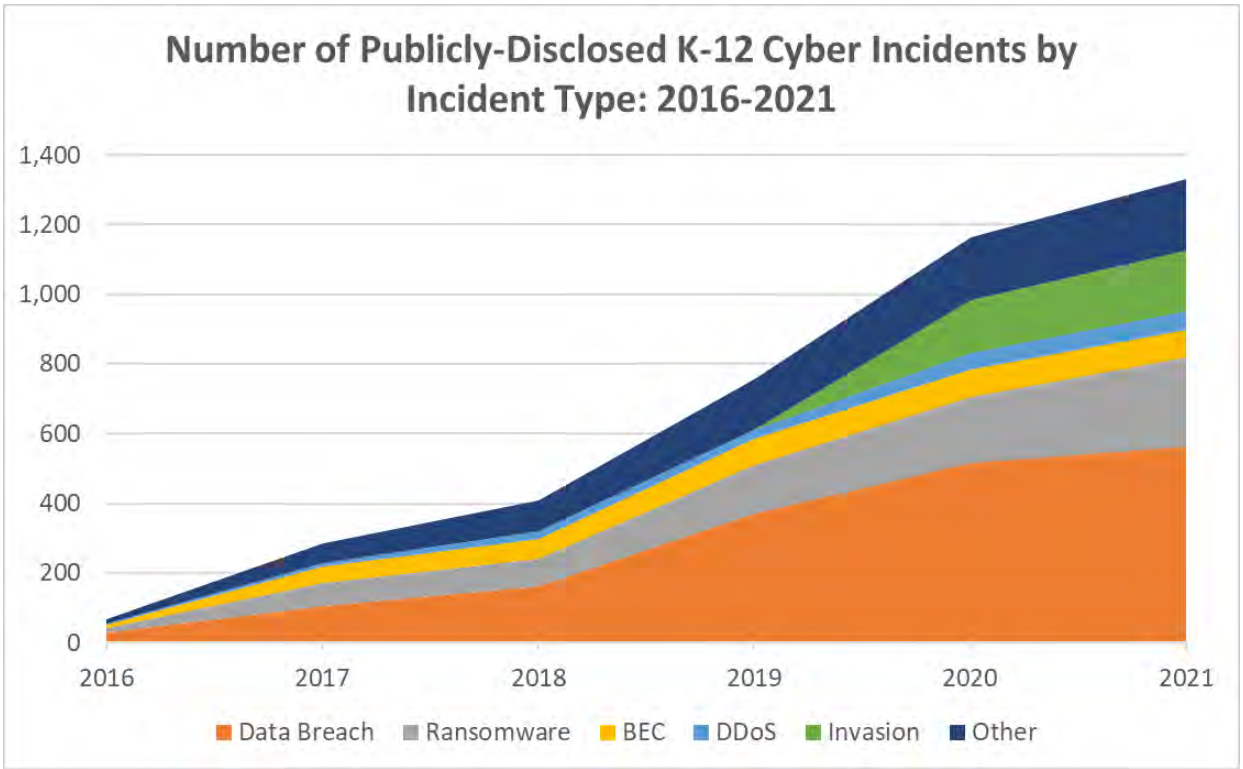
Source: Cedar Attanasio, Cedar (February 1, 2022). "Hackers prey on public schools, adding stress amid pandemic" Associated Press. Available online at: https://apnews.com/article/coronavirus-pandemic-technology-health-business-hacking-aecb37a35f3677e4f2cc62362a23defa

K-12 CYBER INCIDENTS: ANALYSIS AND TRENDS

Since 2016, the K-12 Cyber Incident Map has cataloged a total of 1,331 publicly disclosed school cyber incidents affecting U.S. school districts (and other public educational organizations) across a wide array of incident types, including:

- Student data breaches
- Data breaches involving teachers and school community members
- Ransomware attacks
- Business email compromise (BEC) scams
- Denial of service (DoS) attacks
- Website and social media defacement
- Online class and school meeting invasions
- Other incidents

Averaged over the last six years, this equates to a rate of more than one K-12 cyber incident per school day being experienced by the nation's public schools.



Who is responsible for these incidents and why do they keep occurring? Actors both internal and external to school communities share responsibility:

- School community members—including teachers, administrators, and school board members—who may lack the training and guidance necessary to avoid the errant sharing of personal data and credentials
- Tech-savvy students, who—in the absence of mentoring and adult guidance—may attempt to circumvent existing cybersecurity controls and/or be lured into parlaying their legitimate access to school IT systems to disrupt, cheat, or even cause harm to others
- School suppliers and vendors, whose security practices are not adequately considered during school district procurement decisions and product/service implementation
- Online criminals—some based in the U.S., but many based overseas—who seek to profit from weak school district cybersecurity controls by stealing or extorting money from school districts, their employees, and vendors or via credit and tax fraud enabled by stealing personally identifiable information from school districts. Two types of criminal hackers prey on schools:
    - Those pursuing 'soft targets'—though not specifically schools or school personnel—via mass phishing campaigns and broad-based internet scans for unpatched and unsecured servers
    - Those who specifically target school districts for attack, as evidenced by their sophisticated use of information about school district personnel, communications, vendors, and other operational details to carry out their schemes

While risk management—including digital risk—is a core task of local school system governance, the absence of meaningful cybersecurity risk management standards for schools at either the state or federal levels—coupled with a lack of resources dedicated to meeting any such standards—all but guarantees that many districts will continue to place the safety and security of students, teachers, and community members at avoidable risk.

The 2021 Calendar Year in Focus

During calendar year 2021, the K-12 Cyber Incident Map cataloged a total of 166 school incidents affecting schools in 162 school districts across 38 states. Compared to the prior two years, this represents a decrease in publicly-disclosed incidents—a finding that will be counter-intuitive to many.[4] Three factors may help explain this year-over-year decline.

First, the response to the COVID pandemic—including the unanticipated need to shift to remote learning—may have temporarily inflated the number of cyber incidents experienced by school districts. Indeed, it did give rise to a whole new class of incidents: online class and meeting invasions (known colloquially—though not accurately—as 'Zoombombing').[5] Returning to normal district operations may have helped districts to better protect their communities.

Second, in seeking to shift cybersecurity risk to private insurers, school districts are being forced not only to pay dramatically higher premiums but also to implement commonsense cybersecurity controls—such as multifactor authentication for employees—for the first time. Thanks to this market dynamic and heightened awareness of the cybersecurity challenges facing the K-12 sector in general, school districts

may have done a modestly better job of defending their communities from cybersecurity threats during 2021.[6]

Third, by and large, public-disclosure requirements for school districts and their vendors are quite weak. If it were not for the public interest reporting of security researchers and investigative reporters during 2021—employing, e.g., freedom of information requests to compel districts to share incident details they sought to keep from the public eye—the number of publicly-disclosed incidents cataloged by the K-12 Cyber Incident Map during the past year would have been even smaller. The lack of more robust K-12 cyber incident public disclosure requirements only serves to obscure the realities of school district and vendor operations from those charged with oversight, and to place school community members at unnecessary risk. As such, the smaller number of incidents reported during 2021 may instead reflect a concerning shift away from public disclosure, undermining the ability of independent researchers—and the policymakers and school system leaders who rely on their work—to accurately assess trends and issues.

District Takes "Extraordinary Steps" to Avoid Public Disclosure

As reported by Scott Travis of the *South Florida Sun Sentinel*, the Broward County School District "took extraordinary steps" to keep the public, including 50,000 potential data breach victims, from learning about a March 2021 ransomware attack perpetrated by the Conti ransomware gang, including:

- Waiting 5 months to report key information to affected individuals as well as to the U.S. Department of Health and Human Services, 3 months longer than a federal rule allows. The department is investigating the district's response.
- Communicating to the public that it had conducted its own investigation into the cyber incident but later claiming the findings of the investigation were never put in writing.
- Employing a public relations firm to help dodge questions from the news media and persuade the public that personal data wasn't at risk.
- Rejecting a public records request for emails related to the ransomware incident, with a district lawyer saying "it is not worth any of our time" to review the emails to see if they were exempt under state law.
- Lobbying the Florida state legislature for a law that would keep school district cybersecurity investigations hidden from the public.

Source: Scott Travis (February 17, 2022). "Investigation: Broward schools took extraordinary steps to hide key details of massive data breach." South Florida Sun Sentinel. Available online at: https://www.sun-sentinel.com/news/education/fl-ne-broward-schools-hacker-investigation-report-20220217-6jy2t5rzrzbjxn63oyq5wwuyb4-story.html

Shedding Light on K-12 Cyber Incidents

During 2021, public interest reporting was instrumental to revealing details about K-12 cyber incidents that would have otherwise avoided public disclosure. The work of several researchers and investigative reporters is worthy of special attention:

- Kevin Collier and colleagues at NBC News, who collected and analyzed school files posted on the dark web and found it littered with the personal information of students ("Hackers are leaking children's data — and there's little parents can do." Available online at: https://www.nbcnews.com/tech/security/hackers-are-leaking-childrens-data-s-little-parents-can-rcna1926).

- Dissent Doe, the pseudonym of a privacy advocate and activist who regularly blogs about privacy and cybersecurity incidents—including those affecting U.S. K-12 schools—at https://www.databreaches.net.

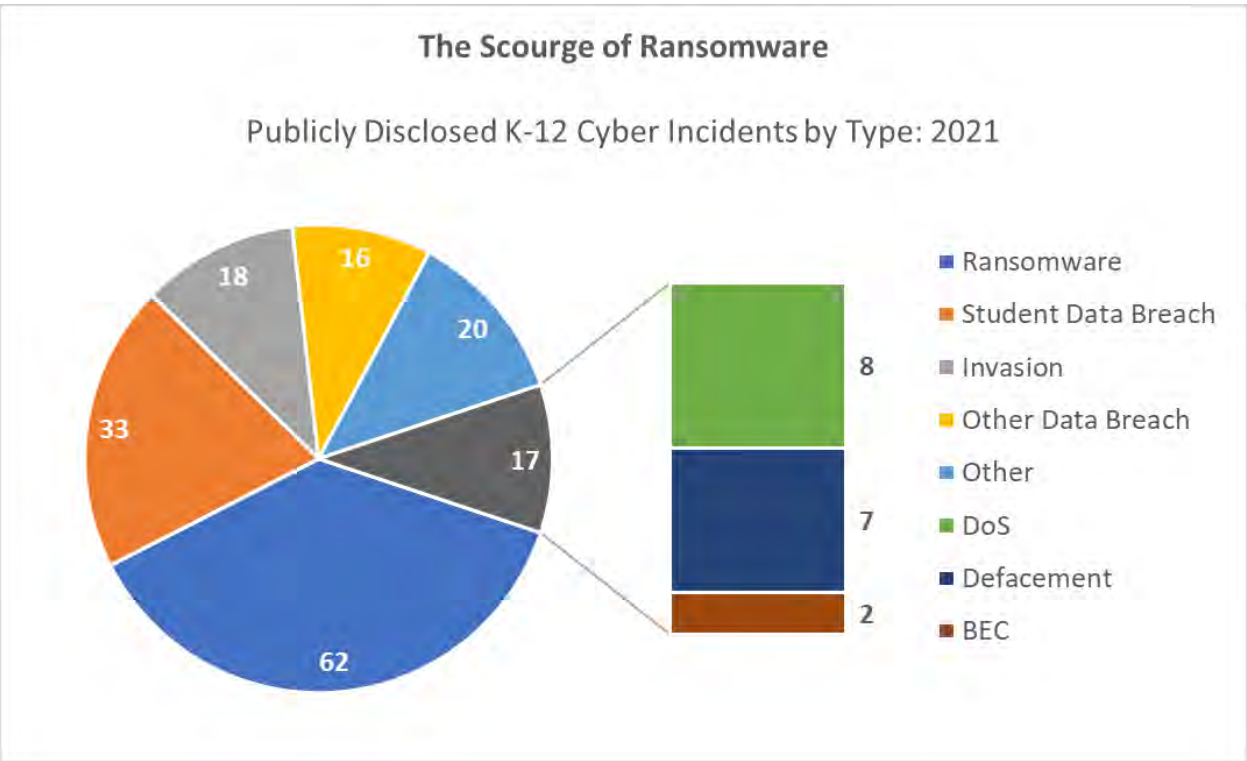
- Grace Ferguson of the *Daily Dot*, who submitted public records requests to 15 school districts across the country to learn more about the impact of K-12 ransomware incidents ("Schools across the nation are getting hit with ransomware attacks—but they won't admit how much it's costing them." Available online at: https://www.dailydot.com/debug/ransomware-public-schools-foia/).

- Dana Kozlov and CBS 2 Chicago colleagues, who submitted public records requests to 60 Illinois school districts asking for correspondence about cyber incidents ("Student And Staff Data From Area School District Were Dumped On The Dark Web, And Parents And Staffers Had No Clue." Available online at: https://chicago.cbslocal.com/2021/09/21/student-staff-data-palos-school-district-dumped-dark-web-caught-off-guard/).

- Brian New and CBS 21 Dallas Fort-Worth colleagues, whose investigative work identified 67 school districts across Texas that had have suffered at least one cybersecurity incident—many of which had previously been undisclosed ("Has Your Kid's Texas School District Been Hammered By Cyberattacks? I-Team Investigation." Available online at: https://dfw.cbslocal.com/2021/08/16/dozens-texas-school-districts-hammered-cyberatacks-ransomware/).

- Julie Watts and CBS 13 Sacramento colleagues, who uncovered "alarming school cyber-attack statistics and a lack of school policies for tracking and reporting these attacks" among California school districts ("Schools Aren't Required to Report Increasing Cyber Attacks: Kids at Risk, Parents in The Dark." Available online at: https://sacramento.cbslocal.com/2021/09/29/school-report-increasing-cyber-attacks-kids-risk-parents/).

What were the most frequently experienced types of school-related cyber incidents reported during 2021? As in prior years, during 2021 school districts experienced a wide array of incident types, including ransomware, data breaches (primarily involving student data), and class and meeting invasions. However, for the first time ever, ransomware incidents were the most frequently disclosed incident type.



The Scourge of Ransomware

During 2021, the K-12 Cyber Incident Map documented 62 instances of U.S. public K-12 school districts being victimized by ransomware, a highly disruptive cyber-attack tactic employed by online criminals to extort money from victims. Incidents were geographically dispersed, with reports of school ransomware emerging from districts of varying sizes across 24 different states.

This is the third straight year that there have been more than 50 publicly disclosed K-12 ransomware attacks and the first year it was the most frequently experienced type of cyber incident cataloged by the K-12 Cyber Incident Map. While the increasing frequency of ransomware attacks should be alarming to K-12 leaders and policymakers, the evolving—and increasingly damaging—tactics of ransomware gangs are primarily what sets 2021 apart from prior years.

While many public reports are ambiguous, the names of ransomware gangs most associated with attacks against U.S. public schools during 2021 included 'PYSA,' 'DoppelPaymer/Grief,' and 'Vice Society.' For their part, the U.S. Federal Bureau of Investigation (FBI) issued an alert specifically warning of the gang behind PYSA ransomware[7] targeting U.S. K-12 educational institutions in March 2021, writing:

> *FBI reporting has indicated a recent increase in PYSA ransomware targeting education institutions in 12 US states and the United Kingdom. PYSA, also known as Mespinoza, is a malware capable of exfiltrating data and encrypting users' critical files and data stored on their systems. The unidentified cyber actors have specifically targeted higher education, K-12 schools, and seminaries. These actors use PYSA to exfiltrate data from victims prior to encrypting victim's systems to use as leverage in eliciting ransom payments.*[8]

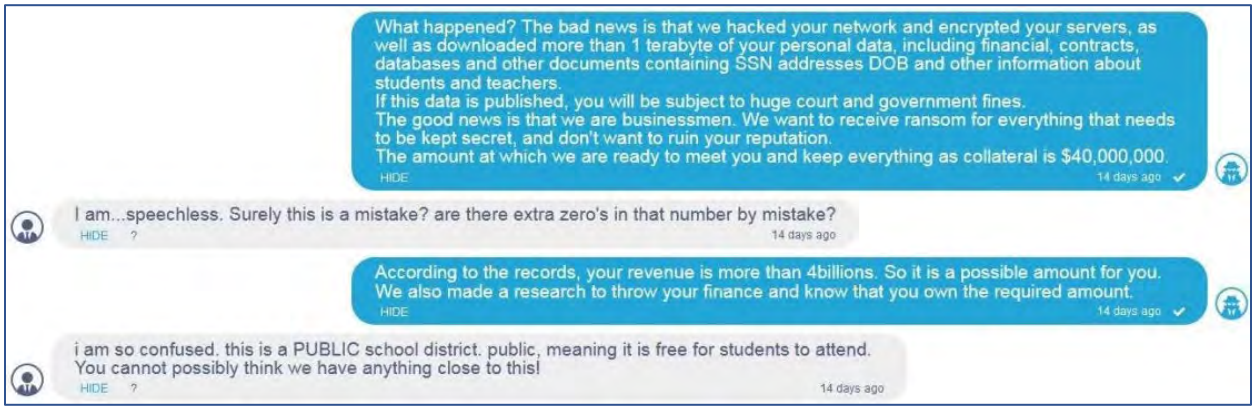
Continuing a trend first observed in 2019, ransomware attacks against school districts commonly resulted in class cancellations and districtwide closures. For instance, during 2021 a Missouri school district was forced to cancel classes for two days as part of their ransomware recovery process which "close[d] down the internet altogether, including the district's phones, paging systems, and security cameras."[9] Further highlighting the challenge of school district resiliency to these attacks, an Oregon school district was forced to distribute printed 'activity packets' to students in an effort to supplement learning while it attempted to recover from its incident:

> *Now with teacher, administrator and student logins all dependent on district domains and portals, the [ransomware attack]… has ground instruction and internal operations to a halt at the district of more than 6,000 students.*[10]

While school districts are often reluctant to disclose whether they (or an insurance company on their behalf) may have been successfully extorted by ransomware gangs, such public disclosures are not unheard of. For instance, in responding to a June 2021 ransomware attack a Texas school district paid $547,045.61 to "protect sensitive, identifiable information from being published." It went on to say:

> *While these are funds that we would have rather spent on the needs of our employees, students and their families, there was no other choice for the district to ensure your safety – our number one priority.*[11]

Even in cases where school districts don't pay a ransom, short- and medium-term unbudgeted remediation costs can be staggering. According to Baltimore County (MD) Public Schools officials, the cost of ongoing recovery from a Ryuk ransomware attack late in 2020 grew to nearly $9.7 million dollars



Excerpts of a conversation between a Broward County Public Schools official and a member of a criminal ransomware gang posted to the gang's blog

Source: Collier, Kevin (April 12, 2021). "Parents were at the end of their chain — then ransomware hit their kids' schools." NBC News. Available online at: https://www.nbcnews.com/tech/security/parents-end-chain-ransomware-hit-rcna646

one year later.[12] In New York, the Buffalo School Board approved spending nearly $9.4 million on external IT consultants to respond to the ransomware attack it suffered in March 2021.[13]

Ransomware gangs continue to evolve their tactics to put pressure on victims to meet their extortion demands. For instance, first documented in last year's 'State of K-12 Cybersecurity' report, ransomware gangs are now routinely employing so-called 'double extortion' tactics against school districts:

> *With this tactic, ransomware actors steal a victim's data before their malware strain activates its encryption routine. They then have the option of demanding two ransoms. The first one is the provision of a decryption utility. The second one guarantees verbal confirmation of having deleted the victim's data from their servers. They can also leverage that data theft to pressure victims — even those that have a robust data backup strategy.*[14]

The experience of Weslaco Independent School District (TX), a late 2020 victim of a ransomware attack, is typical of this double extortion tactic:

> *…the hackers, spurned by Weslaco's decision to not pay, dumped the files they pilfered on their website. One of those, still posted online, is an Excel spreadsheet titled "Basic student information" that has a list of approximately 16,000 students, roughly the combined student population of Weslaco's 20 schools last year. It lists students by name and includes entries for their date of birth, race, Social Security number and gender, as well as whether they're an immigrant, homeless, marked as economically disadvantaged and if they've been flagged as potentially dyslexic.*[15]

Not satisfied with double extortion tactics, ransomware gangs have even resorted to triple extortion of school districts: reaching out to parents directly to encourage them to drive their school districts back to a negotiating table from which they had reportedly walked away:

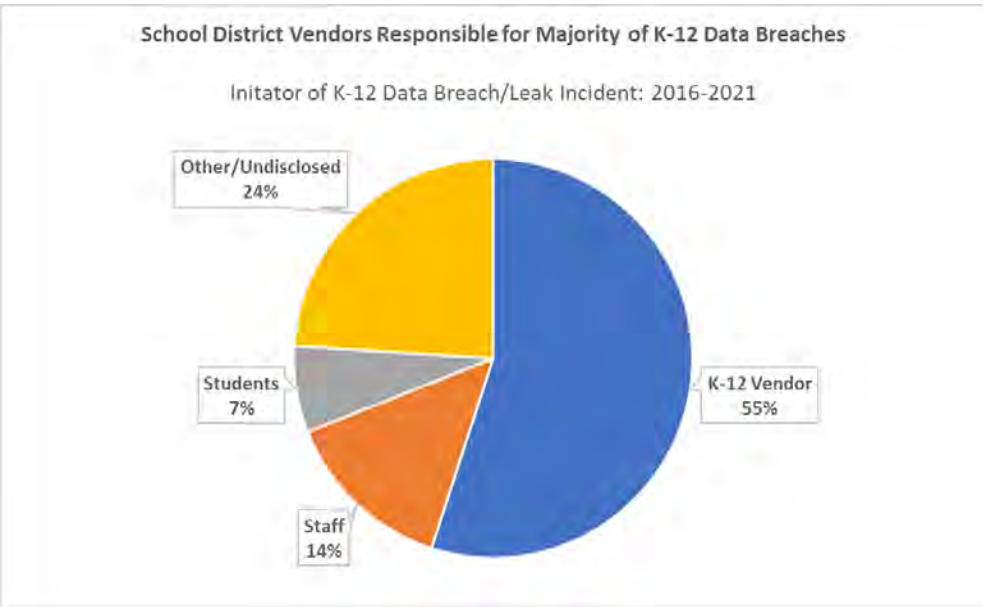
> *Allen ISD was first hacked in September when their phones, WiFi, and printer systems all went down, but say no sensitive information was stolen. However, now parents are coming forward saying they're being threatened by those same hackers.*
>
> *Phil Carpenter, is one of many parents who received an email stating sensitive information has been collected from the district. "[the hackers] claim to have a log of sensitive data from Allen ISD," Carpenter said. "That they have hacked into a lot of the IT resources. It does seem to be some sort of phishing attempt." The email claimed to have control of Allen ISD's network.*
>
> *Another version of the email his wife received, tells parents their school district has five days to send them their demanded payment, or their demand will go up to $10 million. If the money isn't received, the hackers say parents risk having sensitive student information published.*
>
> *For parents it's worrisome.*[16]

Breaches and Leaks of Confidential Student and Teacher Information

School districts and their vendors are routinely the subject of data breaches and leaks involving the confidential information of current and former students and staff. As in previous years, most publicly disclosed K-12 data breach incidents involve student data, but a significant number include teacher and other school data in addition or instead.

The most significant vector for student and teacher data breaches—in terms of numbers of individuals affected—remain school district vendors and other trusted non-profit and government partners. During 2021, school districts reported significant breaches of personal information by: ACT,[17] PCS Revenue,[18] Student Transportation of America,[19] Independent Health,[20] and the Public School and Education Employee Retirement Systems of Missouri.[21]

It is important to note that reports of vendor security issues and vulnerabilities affecting school district IT systems cannot always be directly attributed to K-12 cyber incidents. During 2021 for instance, significant vulnerabilities were disclosed in Netop Vision Pro Education[22] software and Verkada surveillance cameras,[23] as well as in several popular proprietary and open-source software applications commonly used by schools.[24]



While students and school staff generally have little recourse under the law for a data breach incident (no matter the root cause), stockholders and other investors in education companies are granted greater protections in cases where those companies are negligent or materially misstate the potential impact of cyber incidents on their current or future operations. The cease-and-desist order—and accompanying $1 million penalty—issued by the U.S. Securities and Exchange Commission to the education company Pearson in August 2021 is illustrative:

> *Pearson, a multinational educational publishing and services company, made material misstatements and omissions regarding a 2018 cyber intrusion that affected several million rows of student data across 13,000 school, district, and university AIMSweb 1.0*

> *customer accounts in the United States. In its July 26, 2019 report furnished to the Commission, Pearson's risk factor disclosure implied that Pearson faced the hypothetical risk that a "data privacy incident" "could result in a major data privacy or confidentiality breach" but did not disclose that Pearson had in fact already experienced such a data breach. On July 31, 2019, approximately two weeks after Pearson sent a breach notification to affected customers, in response to an inquiry by a national media outlet[25], Pearson issued a previously-prepared media statement that also made misstatements about the nature of the breach and the number of rows and type of data involved.[26]*

The fact that data breaches and other security incidents continue to plague school district vendors and their partners should raise significant questions about the sufficiency and effectiveness of both industry self-regulatory efforts and existing data privacy and security regulations.[27] Indeed, the U.S. Government Accountability Office has recognized "cyberattacks carried out directly against ed-tech vendors…tend to have an especially severe impact on K-12 because they affect a large swath of students across multiple school districts at the same time."[28]

Another significant source of K-12 data breaches are school district staff and school board members, who—whether due to a lack of training or lax cybersecurity controls—inadvertently share personal information of students and/or staff in the course of their duties. This may be in preparation for a school board meeting,[29] in responding to a freedom of information request,[30] or in regular communications with parents and other members of the school community.[31] In perhaps the most politicized data breach incident of 2021, the Governor of Missouri accused a journalist of hacking the Missouri Department of Elementary and Secondary Education website and improperly accessing social security numbers of teachers across the state.[32] Further investigation revealed that:

> *The site, which has both a public side and a secure side available only to certain school-district employees, featured a search tool to look up educators' qualifications and backgrounds. Officials interviewed during the course of the investigation said that as a member of the media, [the journalist] would've only had access to the public-facing portal. But the HTML code for the search tool revealed that Social Security numbers were not encrypted. With records dating back to 2005, an estimated 576,000 teachers' information may have been exposed…. An ITSD application developer and client manager later told state police investigators that data on the teacher lookup website should've been encrypted and that the site is now being redesigned to shield individuals' private information. But the officials also said that in the 10 years since the site was launched, no one in the state's IT division had noticed.[33]*

The final group of individuals commonly responsible for school data breaches—for which information is publicly available—are students themselves. In stories reminiscent of famous movie scenes, every year reports emerge of students who compromise school IT systems, often facilitated by weak school district password policies and a lack of multifactor authentication.

Take the case of Dallas Independent School District (DISD), which announced it was a victim of a massive data breach in September 2021 affecting 800,000 current and former students, staff, and parents:[34]

> *"The confidentiality, privacy, and security of information in our care is one our highest priorities," the district said in the news release. "We take this matter very seriously and have invested significant resources to protect sensitive data. Despite our efforts, the district is now one of a growing number of public and private organizations experiencing cyberattacks."*[35]

What the district did not disclose at the time—and later only emerged through the investigative reporting of Tanya Eiserer and WFAA Dallas colleagues—was that the source of the breach was not a cyber criminal operating overseas, but two DISD students.

> *…the incident was concerning enough to [the district's]…chief information security officer that he quit, and blasted the district's handling of the breach in his resignation email.*
>
> *"I am afraid the details of the breach will become public at some point, and Dallas ISD will lose credibility," [he] wrote… on Oct. 28. "I am now convinced that Dallas ISD IT cannot keep our data safe...."*[36]

While the DISD superintendent resigned following this incident, he did recently accept a national award for "championing the use of technology to enhance teaching and learning" during his tenure.[37]

Other K-12 Cyber Incident Types Disclosed During 2021

While ransomware and data breach incidents are more frequently experienced by school districts, they routinely fall victim to a wide array of other types of incidents. The most common of these include:

- **Business email compromise (BEC) scams**: Involving the use of email to scam school business officials and staff members out of sensitive information and/or millions of dollars of money, including by issuing fake invoices to districts,[38] by redirecting authorized electronic payments to bank accounts controlled by criminals,[39] and by stealing W-2 tax information of district employees.[40]

- **Online meeting and class invasions**: Involving unauthorized access to online classes and K-12 meetings for the purpose of disruption—often by hate speech; via the sharing of shocking images, sounds, and videos; and/or, threats of violence. Despite the attention drawn to these incidents—and availability of advice on how to defend against them—school districts continued to fall prey to these incidents during 2021.[41]

- **Email invasion**: Involving the compromise of a school district's email systems by unauthorized individuals for the purpose of bulk sharing of or links to disturbing images, videos, hate speech, and/or threats of violence to members of the school community.[42]

> *"My heart breaks for anyone who was hurt reading this email this morning and for anyone falsely implicated," [the Superintendent of Bay District Schools]…said. "We know the sentiments expressed in the email do not reflect the values of our school system or our community and I sincerely hope the actual sender is identified quickly."*
>
> Source: The News Herald Staff (July 20, 2021). "Some Bay County students and teachers received the same racist email today. How and why?" The News Herald. Available online at: https://www.newsherald.com/story/news/crime/2021/07/20/bay-county-schools-investigating-racist-email-sent-staff-students/8025767002/

- **Website and social media defacement**: Involving unauthorized changes—such as posting inappropriate language and images—to a school website or official social media account.[43]

- **Denial of service (DOS) attacks**: Intended to make school IT resources unavailable to students and staff by temporarily disrupting their normal functioning.[44]

"Tirthankar Ghosh, the associate director of the University of West Florida Center for Cybersecurity, said distributed denial of services attacks like the one on the [Pinellas County] school system are common and generally of low sophistication.

"The scale of this attack, it really stood out," Ghosh said. "A denial of service attack is pretty common but the fact that 145 schools, their networks came down, that says something."

Source: Ellenbogen, Romy and Fiallo, Josh (May 28, 2021). "St. Petersburg High student's hack crashed internet for all 145 Pinellas schools." Tampa Bay Times. Available online at: https://www.tampabay.com/news/crime/2021/05/28/st-petersburg-high-school-student-crashed-pinellas-schools-systems-internet-with-hack/

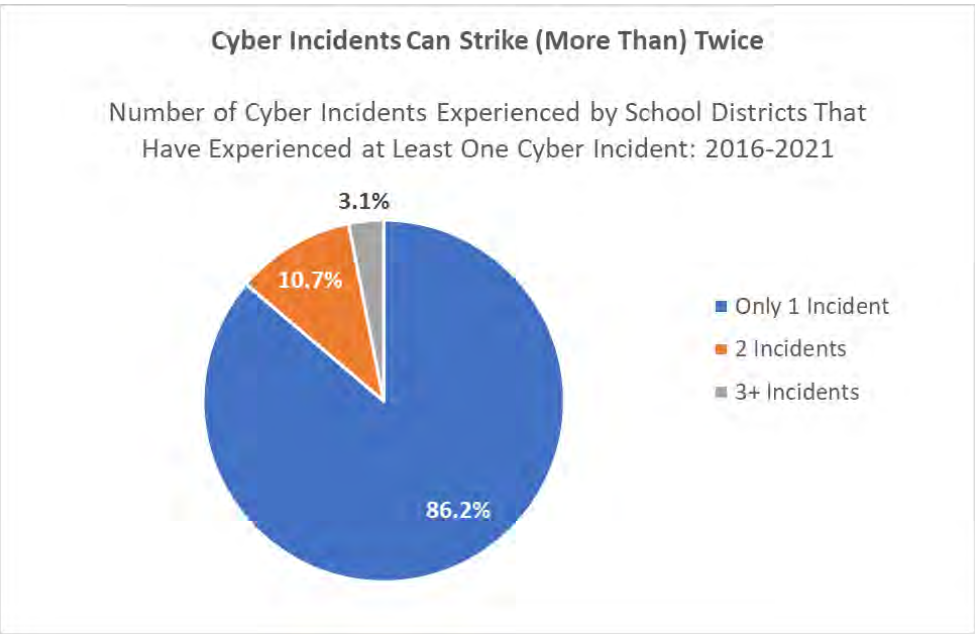
"TECHNOLOGY IS JUST AS IMPORTANT TO THE LEARNING EXPERIENCE IN 2022 AS HEAT IN THE DEPTHS OF WINTER. SO, THE PUBLIC ALSO NEEDS TO KNOW HOW THE SCHOOL SYSTEM WILL PREVENT A SIMILAR CYBERATTACK INCIDENT FROM OCCURRING AGAIN. THE SCHOOL BOARD SHOULD KNOW, TOO, WHETHER IT CAN TAKE STEPS TO PREVENT DIFFERENT AND MORE SEVERE ATTACKS FROM HAPPENING."

Source: Salisbury Post Editorial Board (February 13, 2022). "Editorial: RSS' cyberattack still plaguing systems." Available online at: https://www.salisburypost.com/2022/02/13/editorial-rss-cyberattack-still-plaguing-systems/

CHARACTERISTICS OF DISTRICTS AT RISK

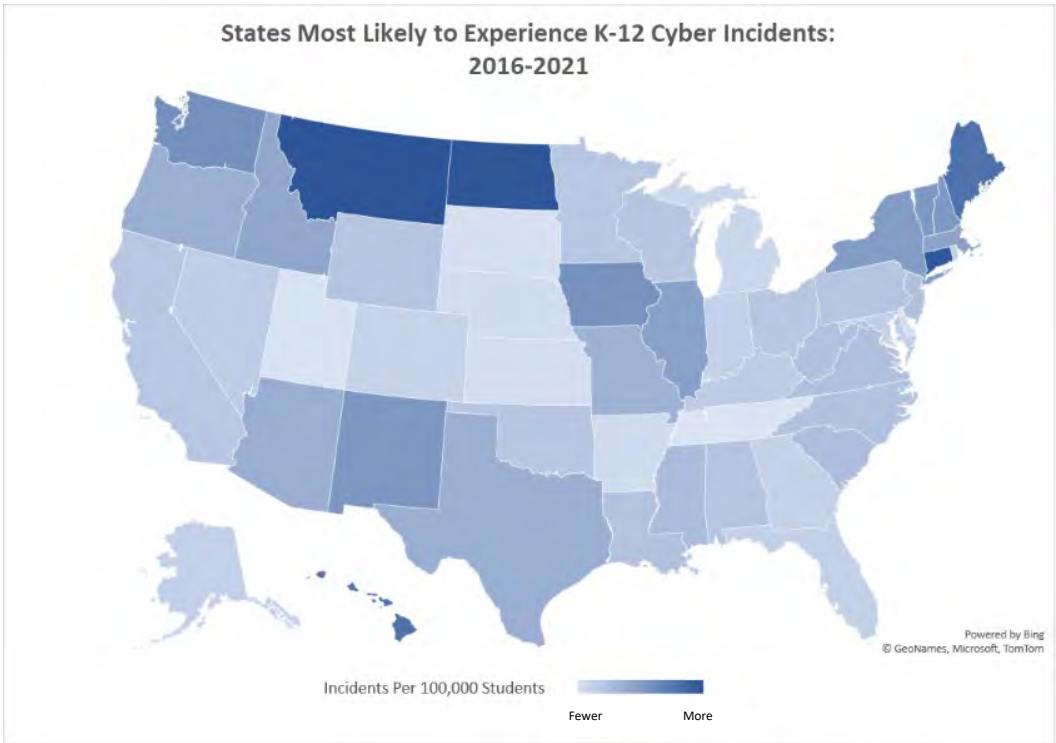
For the 6-year period from 2016-2021, there were a total of 1,331 publicly disclosed K-12 cyber incidents involving 1,123 school districts and other public education agencies.

Of these, 155 school districts—representing nearly 14 percent of school districts and other public education agencies cataloged by the K-12 Cyber Incident Map—have experienced more than one incident. Whether experiencing multiple incidents is a sign of poor cybersecurity risk management practices or just bad luck (or some combination of the two) is beyond the scope of what can be addressed by this dataset, although in cases where districts have experienced five, six, or even more incidents over this period it is suggestive of a story to be told.

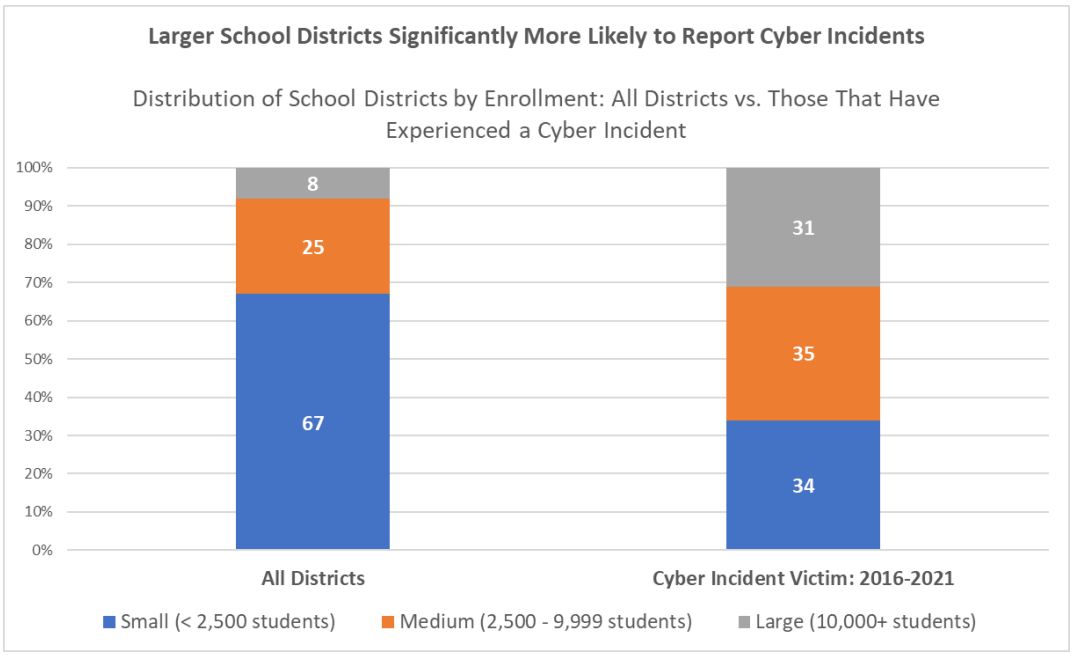


School districts in all 50 states and the District of Columbia (DC) have been cataloged on the K-12 Cyber Incident Map. Not surprisingly, school districts in states with larger student enrollments—including Texas, California, New York, Illinois, and Washington, respectively—are more likely to have experienced K-12 cyber incidents than smaller states over the past six years.

A different picture emerges, however, when controlling for student enrollment. By assessing the rate of K-12 cyber incidents per 100,000 students, what becomes evident is that states such as Montana, North Dakota, Connecticut, Maine, and Hawaii may be experiencing more than their expected share of K-12 cyber incidents.



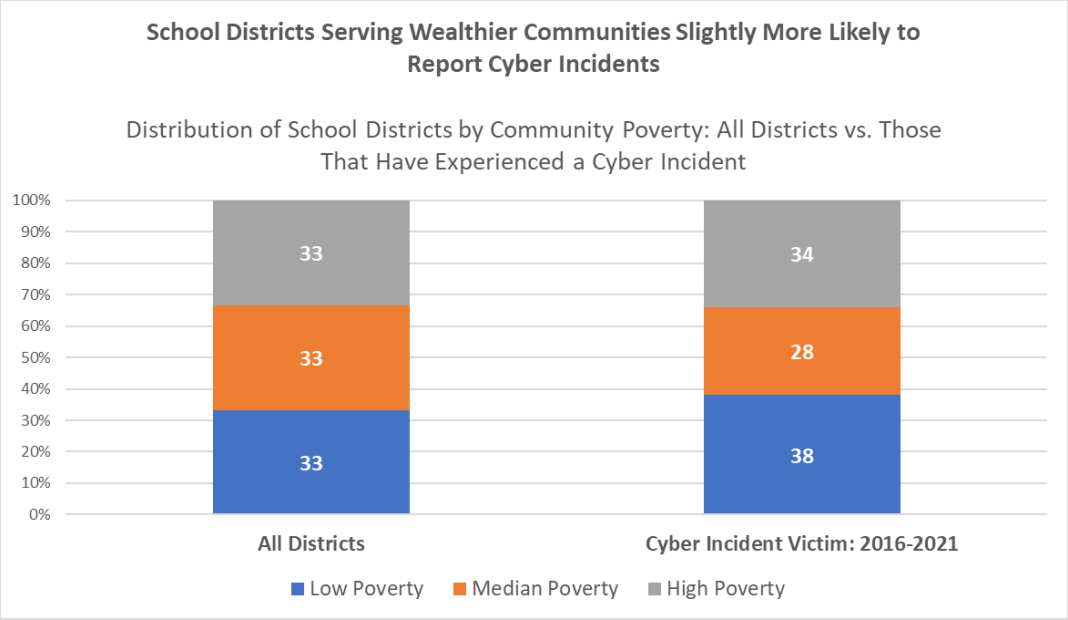
By comparing those districts that have experienced one or more publicly disclosed cyber incidents to all districts nationally, two other themes emerge about the types of school districts at risk of cybersecurity incidents. First, larger school districts (as defined by student enrollment) appear to be at a significantly greater risk for experiencing a cyber incident than small school districts.



There are a few reasons that might explain this pattern in K-12 Cyber Incident Map data. First, larger school districts manage more technology devices and more complex systems than smaller enrollment districts and have more students and employees using that technology. They may also be subject to more directed attacks because they have larger budgets. Smaller enrollment translates to offering a smaller threat profile to malicious actors and a lower chance of a being affected by user actions (whether intentional or by mistake).

Second, incidents that occur in smaller school districts may be less likely to become publicly disclosed than in larger school districts. Hence the fact that they appear to be experiencing fewer incidents may be an artifact of the data collection method used by the K-12 Cyber Incident Map. This may be due to greater media coverage being provided about larger school districts or to the fact that smaller districts may be more limited in terms of their capacity to identify incidents (like data breaches) in a timely manner or at all. Further research would be needed to answer these and related questions.

The second theme that emerges by comparing those districts that have experienced one or more publicly disclosed cyber incidents to all districts nationally is that school districts serving relatively wealthier communities are slightly more likely to have experienced an incident than those serving poorer communities.



Whether this is a function of more frequent public disclosure of K-12 cyber incidents in wealthier communities or that school districts serving relatively wealthier communities may employ more technology for teaching, learning, and school operations than other districts remains unclear.

Nonetheless, it would be a mistake to draw the lesson that school districts in certain states or of certain types or profiles are not at risk from a cyber incident. School districts from all 50 states have suffered significant cyber incidents, from very small, rural districts to the largest urban school districts in the nation. The more important question is what steps can be taken to reduce both the frequency and severity of future K-12 cyber incidents.

SUMMARY AND RECOMMENDATIONS

Since 2016, the K-12 Cyber Incident Map has cataloged a total of 1,331 publicly disclosed school cyber incidents affecting millions of current and former students and teachers in 1,123 U.S. school districts and other public education agencies across all 50 states. Of this total, 166 new incidents were identified over the course of 2021 alone. Averaged over the last six years, this equates to a rate of more than one K-12 cyber incident being disclosed per school day by the nation's public schools.

Given increasing reliance on technology for school district operations, there is every reason to expect that absent significant intervention cyber incidents will continue to plague school districts, placing members of the public at significant—and avoidable—risk.

Existing at the intersection of the K-12 education and cybersecurity sectors, the K12 Security Information Exchange (K12 SIX) is uniquely positioned to both diagnose and point the way toward collective actions that would help stem the rising tide of school cybersecurity risks. Several needs are clear:

- **The need for more and better information sharing about K-12 cyber incidents**. Absent mandated incident disclosure, many school district leaders have demonstrated a lack of willingness to be forthright about cyber incidents with community members and other stakeholders. Yet, when thoughtfully navigated, there are myriad benefits to disclosure: (1) it can assist law enforcement in identifying and prosecuting criminals; (2) it facilitates research to inform policy decision making and the development of K-12 specific cybersecurity guidance and tools; (3) it allows other school districts to take proactive measures to defend themselves from copycat incidents; and, (4) it allows school community members to take steps to protect themselves in a timely manner when they may be at heightened risk personally due to an incident.

- **The need for school districts and other K-12 education agencies to implement commonsense, baseline cybersecurity controls**. Based on the evidence assembled by the K-12 Cyber Incident Map—in conjunction with K-12 specific alerts issued by the FBI and the Cybersecurity and Infrastructure Security Agency (CISA)—it is possible to delineate a small set of cost-effective essential protections that if implemented could dramatically improve the cybersecurity posture of all school districts from the most common threats they are facing. K12 SIX identified this very need and published national cybersecurity standards for school districts—including a free and private school district self-assessment—in the fall of 2021, arguing for a small number of specific controls across four broad categories.[45] Indeed, if the K12 SIX 'Essential Protections' were widely adopted, school districts would fall victim to far fewer cyber incidents and—even in the cases where incidents occurred—school districts would be able to respond and recover more quickly.

- **The need for vendors and suppliers serving the K-12 market to improve their cybersecurity practices**. As the 'State of K-12 Cybersecurity' report series has repeatedly documented, school vendors are responsible for a significant number of the largest K-12 cyber incidents, including

but not limited to student data breaches. Given that school operations are increasingly reliant on outsourced software applications—often hosted off-premises, 'in the cloud'—it is vital that a holistic effort focused not only school district cybersecurity risk management practices and policies, but those of K-12 vendors and suppliers as well, is what will be required to significantly reduce the frequency and severity of cyber incidents experienced by the K-12 sector.

The K12 SIX Essential Cybersecurity Protections[46]

Recommended Protective Measure	Description
1.0 Sanitize Network Traffic to/from the Internet	
1.1 Filter out malware	Block access to known malicious websites
1.2 Campaign against email scams	Reduce the odds that email-based social engineering attacks succeed
1.3 Block malicious documents	Block access to malicious office suite documents, commonly responsible for ransomware
1.4 Limit exposed services	Limit internet exposure of services like remote desktop protocol (RDP)
2.0 Safeguard Student, Teacher, and Staff Devices	
2.1 Restrict administrative access	Keep devices protected and in compliance with security policies
2.2 Apply endpoint protection	Ensure devices used for school remain safe whether used on or off premises
3.0 Protect the Identities of Students, Teachers, and Staff	
3.1 Protect user logins	Implement multi-factor authentication (MFA) to safeguard against compromised passwords
3.2 Improve password management	Prevent password compromise, sharing, and re-use—commonly responsible for data breaches
3.3 Stop online class invasions	Ensure online classes can only be attended by authorized teachers and students
4.0 Perform Regular Maintenance	
4.1 Install security updates	Protect against known vulnerabilities through timely patching of IT systems, computers, and equipment
4.2 Backup critical systems	Build resilience against destructive attacks like ransomware through offline, immutable backups
4.3 Manage sensitive data	Ensure sensitive data is protected, archived, and deleted when no longer needed

See https://www.k12six.org/protective-measures-series for more information about the K12 SIX Essential Protections series of products.

- **The need for cybersecurity threat intelligence, guidance, and best practices *to be tailored specifically for the K-12 sector***, including ensuring it is timely, actionable, and cost-effective. This is especially important given that most school districts do not employ cybersecurity professionals or currently have the capacity to implement with fidelity the dozens of controls

recommended in popular risk management frameworks, such as the National Institute for Standards and Technology (NIST) Cyber Security Framework or the Center for Internet Security (CIS) Controls. In this way, school districts should be thought of as being akin to small- and medium-sized businesses, while being responsible for operating large, complex enterprise IT environments. Moreover, operating as local government agencies, school districts also are subject to sector-specific regulations at both the state and federal levels. Finally, to ensure that threat intelligence and guidance is more likely to be acted on, it is vital that it be communicated to school district leaders via information sources and organizations that are a part of the K-12 sector—such as K12 SIX—and upon which school leaders already rely and trust.

- **The need for school districts and other K-12 organizations to work collectively to address the growing cybersecurity challenge**. If nothing else, the dataset underlying the K-12 Cyber Incident Map demonstrates that U.S. school districts share more in common with each other than not, with respect to the cybersecurity threat landscape. Given limited resources and capacity, it is in the best interests of school district leaders—not just those working in IT positions—to collaborate with each other to increase their schools' resilience to cybersecurity threats. School districts should put a premium on sharing threat intelligence, sharing best practices, developing model policies, pursuing mutually beneficial risk mitigation solutions that can be deployed at scale, and to educating state and federal policymakers about K-12 cybersecurity challenges and potential solutions. While there are many zero- and low-cost steps that individual school districts can and must take now, significant progress won't be made if the burden remains on under-resourced districts working in isolation.

Challenges and Opportunities Ahead

Two sets of actors have the potential to dramatically reshape the K-12 cybersecurity landscape in the near term: cyber risk insurance providers, who have a direct financial incentive to reduce the cybersecurity risks that school districts are facing as a condition of coverage, and policymakers at the state and federal levels, who have an array of proverbial carrots and sticks at their disposal to uplift the cybersecurity risk management practices of the K-12 sector.

Until recently, cyber risk insurance was perceived as a near foolproof safety valve in case of a school cyber incident, such that school district leaders would sometimes purchase insurance in lieu of enacting commonly recommended preventive measures. Take the experience of one Pennsylvania district (as reported in late 2020):

> *The district had two cyberattacks in two years, but avoided paying ransom in both cases.*
>
> *School board members voted Wednesday night to purchase a new cyber liability insurance policy with $2 million worth of coverage, twice what they had last year. The cost of the insurance is $19,000 per year.*
>
> *"It's going to be a policy everyone's going to be looking to get from now on. It's something that 5-10 years ago we wouldn't have even thought about, but now it's a necessity," said [the school district]…business manager.*[47]

From a strictly economic perspective, such a decision could even have been viewed as rational. What school district leaders are beginning to find, however, is that relatively inexpensive school cyber risk insurance is quickly going the way of the dodo. Indeed, those providers still willing to insure school district cyber risks in 2022 are both significantly raising costs and requiring increasingly stringent cybersecurity risk management practices as a precondition for coverage.[48] To the extent that these preconditions are aligned to existing cybersecurity risk management frameworks already employed by forward-leaning school districts, like the K12 SIX Essential Cybersecurity Protections, the more economies of scale could be realized in assisting other school districts to uplift their cybersecurity risk management practices.

While the impact of changes to the K-12 cyber risk insurance market shouldn't be understated, ultimately policymakers will be required to act to accelerate change. After all, as local government agencies, school districts are neither motivated by strictly economic factors nor are they subject to the same type of existential risks as private organizations in the case of catastrophic cyber incidents.

According to the Consortium for School Networking (CoSN), many state and federal policymakers have been actively engaged with issues of cybersecurity with at least indirect relevance to the K-12 sector over the last year.[49] At the federal level, school district leaders would do well to pay particular attention to the enactment of two federal laws passed in 2021:

- *The K-12 Cybersecurity Act*—the first ever federal K-12 specific cybersecurity law—which requires CISA to issue a study of the cybersecurity risks facing the K-12 sector in spring 2022, including recommendations for further actions that could be taken to help schools to better defend themselves[50]

- *The State and Local Cybersecurity Improvement Act*, which authorized the appropriation of $1 billion for grants to state, local and tribal governments—including school districts—to address cybersecurity threats and risks to their IT systems[51]

Coupled with increasing engagement from the U.S. Department of Education—spurred in part by lawmaker requests[52]—there are signs that momentum is building for meaningful federal regulations and resources in support of improved K-12 cybersecurity practices. Nonetheless, careful attention will have to be paid to ensuring that any new regulations and resources lead to meaningful improvements in K-12 cybersecurity risk management practices. Too many students', teachers', and community members' livelihoods are at stake—even if some have been slow to recognize it.

APPENDIX: DATA AND METHODS

The K-12 Cyber Incident Map (https://www.k12six.org/map) and underlying database—currently maintained as a public service by the K12 Security Information Exchange (K12 SIX)—was originally launched in March 2017 as an effort to build an empirical base of information about the state of cybersecurity in U.S. public K-12 schools and districts.[53] While other efforts exist to catalog trends in cybersecurity incidents and data breaches, including in education, none bring a lens that is both vendor-neutral and reliably actionable for U.S. policymakers, K-12 school leaders, and school district IT practitioners.

Widely cited research studies such as Verizon's *Data Breach Investigations Report* series[54] define the education sector overly broadly for purposes useful to targeted domestic action: combining K-12 and postsecondary institutions, public and private institutions, U.S. and global institutions all in a singular category of analysis. Other public sources of data breach incidents compiled by experts exclude the reporting of other significant types of cybersecurity incidents, such as business email compromise and ransomware. While there may be lessons to be drawn from these valuable efforts for education stakeholders, the unique focus of the K-12 Cyber Incident Map has allowed it to become the definitive source of information about the state of K-12 cybersecurity.

The K-12 Cyber Incident Map and underlying database captures detailed information about:

- Publicly-disclosed cybersecurity incidents affecting public K-12 schools, districts, charter schools, and other public education agencies (such as regional and state education agencies) in the 50 states and the District of Columbia, especially those that occur on K-12 managed networks and devices and/or under the direction of school districts
- The characteristics of public school districts (including charter schools) that have experienced one or more publicly-disclosed cybersecurity incidents.

Cyber incidents are defined as those that impact the confidentiality, integrity, and availability of a school district's IT and data systems (whether on-premises or hosted by a vendor working for the district). Whether an incident affects one school or classroom within a district or many—or is due to the actions (or inaction) of a school vendor or partner, including a regional or state education agency—incidents are generally assigned to school districts. This is because school districts (or local education agencies as they are also known) are the primary government entities charged with responsibility for managing taxpayer dollars, employee confidentiality, and student data privacy under state and federal law. As such, when a school vendor or regional/state agency experiences an incident, it is possible that it affects more than one school district and may therefore get reported as more than one incident on the Map. Related incidents are coded as such in the database underlying the K-12 Cyber Incident Map.

By associating incidents with school districts, the K-12 Cyber Incident Map can identify patterns in school district characteristics that may be associated with the odds of experiencing an incident, such as district size and student poverty. School district data are supplemented with select information drawn from the U.S. Department of Education's Common Core of Data, categorized in a manner consistent with that employed by the National Center for Education Statistic's Fast Response Survey System.[55] Similarly,

poverty status of school districts is drawn from the U.S. Census Bureau's Small Area Income and Poverty Estimates (SAIPE).[56]

Data about K-12 cyber incidents are sourced from a large variety of outlets, including state and local governments, law enforcement, press reports, other data breach reporting services and information sharing communities, social media and online forums, self-reports, and tips. While some reports may be ambiguous (and are often incomplete), all are screened for authenticity and relevance before being recorded.

Nonetheless, the database of K-12 cybersecurity incidents is incomplete and only captures a small fraction of incidents experienced by schools, districts, their partners, and vendors. To the degree that there are mandatory cybersecurity incident reporting requirements for K-12 school districts, they vary across states. Required disclosures are often not publicly accessible and/or are limited to narrow categories of cyber incidents (such as data breaches over a certain magnitude). School districts may resist self-reporting if they believe an incident may reflect poorly on their administration. Finally, given a deficit of attention paid to cybersecurity risk management in many school districts, there may also be a considerable gap between when school districts experience an incident and when (or if) they become aware of that fact.

As of December 2019, summary data about K-12 cybersecurity incidents are published on an enhanced, interactive map of the United States via an integration with OpenStreetMap.[57] Incidents on the map are color-coded by 'primary' incident type:

- phishing attacks resulting in the disclosure of personal data (blue icons)
- other unauthorized disclosures, breaches or hacks resulting in the disclosure of personal data (purple icons)
- ransomware attacks (yellow icons)
- denial-of-service attacks (green icons)
- other cyber incidents resulting in school disruptions and unauthorized disclosures (red pins)

Given that incident types can co-occur (e.g., malware delivery via phishing email, resulting in a data breach), reporting by primary incident type should be interpreted with some caution.

NOTES

[1] Institute of Education Sciences, National Center for Education Statistics. "Digest of Education Statistics: Most Current Digest Tables." Washington, DC: U.S. Department of Education. Available online at: https://nces.ed.gov/programs/digest/current_tables.asp

[2] Levin, Douglas A. (2019). "The State of K-12 Cybersecurity: 2018 Year in Review." EdTech Strategies, LLC/The K-12 Cybersecurity Resource Center. Available online at: https://www.k12six.org/s/K12Cybersecurity-2018YIR.pdf; Levin, Douglas A. (2020). "The State of K-12 Cybersecurity: 2019 Year in Review." EdTech Strategies, LLC/The K-12 Cybersecurity Resource Center. Available online at: https://www.k12six.org/s/K12Cybersecurity2019YearinReview.pdf; Levin, Douglas A. (2021). "The State of K-12 Cybersecurity: 2020 Year in Review." EdTech Strategies, LLC/The K-12 Cybersecurity Resource Center and the K12 Security Information Exchange. Available online at: https://www.k12six.org/s/StateofK12Cybersecurity-2020.pdf

[3] U.S. Government Accountability Office (GAO) (September 2020). Data Security: Recent K-12 Data Breaches Show That Students Are Vulnerable to Harm. GAO-20-644. Washington, DC: GAO. Available online at: https://www.gao.gov/products/GAO-20-644

[4] See, Levin, Douglas A. (2020). "The State of K-12 Cybersecurity: 2019 Year in Review." Arlington, VA: EdTech Strategies, LLC/The K-12 Cybersecurity Resource Center. https://www.k12six.org/s/K12Cybersecurity2019YearinReview.pdf; Levin, Douglas A. (2021). "The State of K-12 Cybersecurity: 2020 Year in Review." EdTech Strategies, LLC/The K-12 Cybersecurity Resource Center and the K12 Security Information Exchange. https://www.k12six.org/s/StateofK12Cybersecurity-2020.pdf

[5] As discussed at length in Levin, Douglas A. (2021). "The State of K-12 Cybersecurity: 2020 Year in Review." EdTech Strategies, LLC/The K-12 Cybersecurity Resource Center and the K12 Security Information Exchange. https://www.k12six.org/s/StateofK12Cybersecurity-2020.pdf; see also https://en.wikipedia.org/wiki/Zoombombing

[6] See, e.g., Consortium for School Networking (2021). "EdTech Leadership Survey Report." Available online at: https://emma-assets.s3.amazonaws.com/paqab/2ad6dcd4fb0d923337a5a6d6a5344ee0/Survey_Report_2021_Final.pdf; Project Tomorrow (2021). "Creating a Common Culture of Action Around Cybersecurity." Available online at: https://tomorrow.org/speakup/pdfs/Creating-a-Common-Culture-of-Action-Around-Cybersecurity.pdf;

[7] Gatlan, Sergiu (June 23, 2021). "PYSA ransomware backdoors education orgs using ChaChi malware" Bleeping Computer. Available online at: https://www.bleepingcomputer.com/news/security/pysa-ransomware-backdoors-education-orgs-using-chachi-malware/

[8] U.S. Federal Bureau of Investigation (FBI) (March 16, 2021). "Increase in PYSA Ransomware Targeting Education Institutions." Alert Number CP-000142-MW. Available online at: https://www.ic3.gov/Media/News/2021/210316.pdf

[9] Wehmhoener, Karl (December 7, 2021). "Eldon School District canceled classes Tuesday due to ransomware attack." ABC 17. Available online at: https://abc17news.com/news/2021/12/07/eldon-school-district-cancels-classes-due-to-ransomware/

[10] Manning, Rob (April 27, 2021). "Instruction halted as east Multnomah Co. school district suffers apparent cyberattack." OPB. Available online at: https://www.opb.org/article/2021/04/27/instruction-halted-as-east-multnomah-co-school-district-suffers-apparent-cyberattack/

[11] KENS 5 Staff (August 4, 2021). "'There was no other choice' | Judson ISD pays more than $547,000 following ransomware attack." KENS 5. Available online at: https://www.kens5.com/article/news/local/judson-isd-pays-more-than-547000-following-ransomware-attack/273-4e3d2c4c-657e-47c2-a217-4e8be2079855

[12] Corfield, Gareth (June 16, 2021). "Ryuk ransomware recovery cost us $8.1m and counting, says Baltimore school authority." The Register. Available online at: https://www.theregister.com/2021/06/16/baltimore_ryuk_ransomware_dollars_8_1m_recovery_cost/?&web_view=true; Simpson, Amy (November 24, 2021). "A year later, Baltimore County Schools ransomware recovery costs nearly $9.7 million." WBFF Baltimore. Available online at: https://www.msn.com/en-us/news/us/a-year-later-baltimore-county-schools-ransomware-recovery-costs-nearly-9-7-million/ar-AAR6f3l

[13] Watson, Stephen T (October 18, 2021). "Buffalo School District to Spend $10M on Ransomware Response." Government Technology. Available online at: https://www.govtech.com/education/k-12/buffalo-school-district-to-spend-10m-on-ransomware-response
[14] Bisson, David (December 23, 2021). "Ransomware Attackers' New Tactic: Double Extortion." Security Intelligence. Available online at: https://securityintelligence.com/articles/ransomware-double-extortion/
[15] Collier, Kevin (September 10, 2021). "Hackers are leaking children's data — and there's little parents can do." NBC News. Available online at: https://www.nbcnews.com/tech/security/hackers-are-leaking-childrens-data-s-little-parents-can-rcna1926
[16] Nielsen, Nicole (October 6, 2021). "Allen ISD Parents Concerned About Receiving Cybersecurity Breach Emails." CBS DFW. Available online at: https://dfw.cbslocal.com/2021/10/06/allen-isd-parents-receive-cybersecurity-breach-emails/
[17] New, Brian (August 16, 2021). "Has Your Kid's Texas School District Been Hammered By Cyberattacks? I-Team Investigation." CBS DFW. Available online at: https://dfw.cbslocal.com/2021/08/16/dozens-texas-school-districts-hammered-cyberatacks-ransomware/
[18] Freedman, Linn Foster (April 22, 2021). "School Nutrition Vendor Sued for Compromise of 867,209 K-12 Student Records." Robinson + Cole. Available online at: https://www.dataprivacyandsecurityinsider.com/2021/04/school-nutrition-vendor-sued-for-compromise-of-867209-k-12-student-records/
[19] Cooper, Kenny (September 7, 2021). "Parents outraged after bus company email reveals students' information." WHYY. Available online at: https://whyy.org/articles/springfield-delco-parents-outraged-after-bus-company-email-reveals-students-information/
[20] WGRZ Staff (October 8, 2021). "Williamsville School employees' private health data inadvertently leaked by Independent Health." WGRZ. Available online at: https://www.wgrz.com/article/news/local/private-health-data-of-williamsville-school-employees-inadvertently-leaked-by-independent-health/71-2d476804-2d70-4689-b7c9-d4fb224b54c6
[21] Erickson, Kurt (October 19, 2021). "Missouri teacher pension system probing possible cyber attack." St. Louis Post-Dispatch. Available online at: https://www.stltoday.com/news/local/govt-and-politics/missouri-teacher-pension-system-probing-possible-cyber-attack/article_49c5817e-ac8d-5c88-a581-dc5b5c34d8f0.html
[22] Keierleber, Mark (October 18, 2021). "Popular student monitoring software could have exposed thousands to hacks." Fast Company. Available online at: https://www.fastcompany.com/90686770/netop-student-monitoring-software-hack
[23] Turton, William (March 9, 2021). "Hackers Breach Thousands of Security Cameras, Exposing Tesla, Jails, Hospitals." Bloomberg. Available online at: https://www.bloomberg.com/news/articles/2021-03-09/hackers-expose-tesla-jails-in-breach-of-150-000-security-cams
[24] E.g., PrintNightmare https://en.wikipedia.org/wiki/PrintNightmare; Log4j https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance and https://www.k12six.org/news/k12-six-releases-k12-specific-log4j-collaboration-resource; Fung, Brian (August 24, 2021). "Data leak exposes tens of millions of private records from corporations and government agencies." CNN Business. Available online at: https://www.cnn.com/2021/08/24/tech/data-leak-microsoft-upguard/index.html
[25] Olson, Parmy (July 31, 2019). "Pearson Hack Exposed Details on Thousands of U.S. Students." Wall Street Journal. Available online at: https://www.wsj.com/articles/pearson-hack-exposed-details-on-thousands-of-u-s-students-11564619001
[26] U.S. Securities and Exchange Commission (August 16, 2021). "SEC Charges Pearson plc for Misleading Investors About Cyber Breach." Available online at: https://www.sec.gov/news/press-release/2021-154; SEC Order: https://www.sec.gov/litigation/admin/2021/33-10963.pdf
[27] There is a growing body of best practices and guidance for the management of vendor and supply-chain risk that could be adapted for use in the K-12 education sector. See, e.g., National Institute of Standards and Technology (NIST). "Best Practices in Cyber Supply Chain Risk Management – Conference Materials: Cyber Supply Chain Best Practices." Available online at: https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf; NIST. "Best Practices in Cyber Supply Chain Risk Management – Conference Materials: Organizational Strategies for Cyber Supply Chain Risk Management." Available online at: https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-SCRM-Organizational-Strategy.pdf; NIST. "Notional Supply Chain Risk Management Practices for Federal Information Systems." NISTIR 7622. Available

online at: https://nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7622.pdf; NIST. "Supply Chain Risk Management Practices for Federal Information Systems and Organizations." NIST Special Publication800-161. Available online at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf; NIST. "Key Practices in Cyber Supply Chain Risk Management: Observations from Industry." NISTIR 8276. Available online at: https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8276.pdf

[28] David Saleh Rauf (November 16, 2020). "Cyberattacks on Ed-Tech Companies Rare, But Hugely Disruptive, Report Finds." EdWeek Market Brief. Available online at: https://marketbrief.edweek.org/marketplace-k-12/cyberattacks-ed-tech-companies-rare-hugely-disruptive-report-finds/

[29] See, e.g., Attrino, Anthony G. (June 9, 2021). "N.J. school worker accidentally leaked Social Security numbers of staff to public." NJ Advance Media for NJ.com. Available online at: https://www.nj.com/bergen/2021/06/nj-school-worker-accidentally-leaked-social-security-numbers-of-staff-to-public.html; Gallion, Bailey (May 7, 2021). "Cybercriminals potentially accessed data of 10,000 people in Brevard School Board breach." Florida Today. Available online at: https://www.floridatoday.com/story/news/education/2021/05/07/brevard-county-school-district-warns-10-000-people-data-breach-email-addresses/4995507001/

[30] See, e.g., Horner, Rick (July 23, 2021). "Student private information breached in Fairfax County Public Schools." Fairfax County Times. Available online at: https://www.fairfaxtimes.com/articles/student-private-information-breached-in-fairfax-county-public-schools/article_d8f36b5a-eb17-11eb-b460-bb82b3b50727.html; McConnell, Jim. (April 19, 2021). "School system mistakenly releases names of students, staff with COVID." Chesterfield Observer. Available online at: https://www.chesterfieldobserver.com/articles/school-system-mistakenly-releases-names-of-students-staff-with-covid/; Johnson, Alec (February 4, 2021)."The Shorewood School District is apologizing for accidentally releasing student data." Milwaukee Journal Sentinel. Available online at: https://www.jsonline.com/story/communities/northshore/news/shorewood/2021/02/04/shorewood-school-district-apologizes-releasing-student-data/4355690001/

[31] See, e.g., Salhotra, Pooja (August 12, 2021). "Brooklyn Tech students uncovered a NYC schools data breach. Here's how they took action." Chalkbeat New York. Available online at: https://ny.chalkbeat.org/2021/8/12/22622143/brooklyn-tech-nyc-schools-data-breach; Tooten, Tim (April 13, 2021). "BCPS takes responsibility for data breach that affected teachers." WBAL TV 11. Available online at: https://www.wbaltv.com/article/baltimore-county-public-schools-accept-responsibility-for-data-breach/36109608; KTRK Staff (February 1, 2021). "Friendswood ISD students' Social Security numbers mistakenly sent to school photographer." ABC 13. Available online at: https://abc13.com/friendswood-isd-school-student-social-security-numbers-leak-sent-to-photographer/10221735/; Cross, Ian (November 29, 2021). "Bay Village school district accidentally releases seniors' personal info, including grades, to all families." ABC News 5 Cleveland. Available online at: https://www.news5cleveland.com/news/local-news/oh-cuyahoga/bay-village-school-district-accidentally-releases-seniors-personal-info-including-grades-to-all-families

[32] See, e.g., Treisman, Rachel. (October 14, 2021). "A Missouri newspaper told the state about a security risk. Now it faces prosecution." NPR. Available online at: https://www.npr.org/2021/10/14/1046124278/missouri-newspaper-security-flaws-hacking-investigation-gov-mike-parson

[33] Freed, Benjamin (February 22, 2022). "Missouri website vulnerability was present since 2011, investigation finds." StateScoop. Available online at: https://statescoop.com/missouri-website-vulnerability-was-present-since-2011/

[34] Barber, Katy (February 9, 2022). "Turns out a couple kids were behind a massive Texas school system hack." KTSA. Available online at: https://www.ktsa.com/turns-out-a-couple-kids-were-behind-a-massive-texas-school-system-hack/

[35] Osborne, Ryan (September 3, 2021). "Cyberattack hits Dallas ISD data; current and former students' records could be impacted." WFAA. Available online at: https://www.wfaa.com/article/news/education/cyberattack-dallas-isd-data-breach-hack-current-former-students-records-impact/287-bc42c3ec-1092-4b51-ade0-cbf0d9fdcbb7

[36] Eiserer, Tanya, and Trahan, Jason (February 7, 2022). "'They pretty much had access to everything': WFAA reveals the masterminds behind last year's Dallas ISD cyber breach. And it's not who you think." WFAA. Available online at: https://www.wfaa.com/article/news/local/investigates/wfaa-reveals-masterminds-behind-dallas-isd-cyber-breach/287-15b22b82-b226-424d-9b27-a7d5b5120ac3

[37] AASA (February 18, 2022). "Texas, Utah School District Leaders Recognized for EmpowerED Digital Superintendent Award at AASA's National Conference on Education." Available online at: https://www.aasa.org/content.aspx?id=47626

[38] Meadows, Jonah (November 29, 2021). "ETHS Defrauded Of $48,570 In Hack That Exposed 1,139 Identities." Patch. Available online at: https://patch.com/illinois/evanston/eths-defrauded-48-570-hack-exposed-1-139-identities

[39] Hanna, Maddie and Vella, Vinny (March 4, 2021). "Chester Upland School District says millions of dollars are missing. The DA has launched a probe." The Philadelphia Inquirer. Available online at: https://www.inquirer.com/news/chester-upland-school-district-investigation-delaware-county-20210304.html

[40] Colburn, David (February 17, 2021). "ISD 2142 hit with phishing scheme." The Timberjay. Available online at: http://www.timberjay.com/stories/isd-2142-hit-with-phishing-scheme,17343

[41] See, e.g., Associated Press (February 12, 2021). "School meeting hacked with racial epithet, obscene video." The Washington Times. Available online at: https://www.washingtontimes.com/news/2021/feb/12/school-meeting-hacked-with-racial-epithet-obscene-/; DeNardo, Mike (February 22, 2021). "Police investigate racist hack that disrupted Ben Franklin High students' virtual field trip." KYW Newsradio. Available online at: https://www.audacy.com/kywnewsradio/news/local/police-investigate-hack-that-disrupted-virtual-field-trip; Purvis, Leon (March 4, 2021). "Internet hack, threat disrupt learning in South Hadley." Western Mass News. Available online at: https://web.archive.org/web/20210317210021/https://www.westernmassnews.com/news/internet-hack-threat-disrupt-learning-in-south-hadley/article_750b2bb8-7d31-11eb-9822-0379f7330fa0.html; Maldonado, Zinnia (March 17, 2021). "Waterbury middle school hacked, students exposed to inappropriate content." FOX 61. Available online at: https://www.fox61.com/article/news/crime/waterbury-middle-school-hacked-students-exposed-to-inappropriate-content/520-706d99a2-5a3e-43ea-99d0-456ca7abe5b7; Wagner, Jacob (November 24, 2021). "School board Zoom meeting hacked." The Star. Available online at: https://www.grandcoulee.com/story/2021/11/24/news/school-board-zoom-meeting-hacked/14776.html

[42] See, e.g., Arevalo, Greena (January 8, 2021). "Disturbing email sent to Virginia high school students, parents upset at delayed notification." CBS 17. Available online at: https://www.cbs17.com/news/south/disturbing-email-sent-to-virginia-high-school-students-parents-upset-at-delayed-notification/; Blanchard, Peter (January 25, 2021). "Council Rock Apologizes For 'Inappropriate' Emails." Patch. Available online at: https://patch.com/pennsylvania/newtown-pa/council-rock-apologizes-inappropriate-emails; Eliopoulos, Peter (January 24, 2021). "Thousands in Massachusetts school district receive violent, racist emails from student account." WCVB. Available online at: https://www.wcvb.com/article/thousands-in-gardner-massachusetts-school-district-receive-violent-racist-emails-from-student-account/35301402; Cote, Jackson (March 1, 2021). "Shelter in place ordered at Chicopee Comprehensive High School after public school email system hacked and 'questionable' message received, police say." Mass Live. Available online at: https://www.masslive.com/police-fire/2021/03/shelter-in-place-ordered-at-chicopee-comprehensive-high-school-after-public-school-email-system-hacked-and-questionable-message-received-police-say.html

[43] See, e.g., Wisely, John (March 15, 2021). "Hackers post racist slurs on Troy schools website." Detroit Free Press. Available online at: https://www.freep.com/story/news/education/2021/03/15/hackers-slurs-troy-schools/4706894001/; Scripps staff (March 16, 2021). "Leon County Schools website hacked." WTXL Tallahassee. Available online at: https://www.wtxl.com/news/local-news/leon-county-schools-website-social-media-accounts-hacked; Tarrazi, Alexis (June 24, 2021). "Vulgar Messages Appear As Bridgewater Schools' Websites Hacked." Patch. Available online at: https://patch.com/new-jersey/bridgewater/vulgar-messages-appear-bridgewater-schools-websites-hacked

[44] See, e.g., February 5, 2021. "Winthrop Officials Investigating Cyber Attack on Town, School Servers." Available online at: https://www.town.winthrop.ma.us/home/news/winthrop-officials-investigating-cyber-attack-town-school-servers; Bray, Hiawatha (February 10, 2021). "Hacking attacks plague Massachusetts schools." Boston Globe. Available online at: https://www.bostonglobe.com/2021/02/10/business/hacking-attacks-plague-massachusetts-schools/; Mooney, John (January 21, 2021). "Cyber Attack Causes Disruption of Scotch Plains-Fanwood Schools." Tapinto. Available online at: https://www.tapinto.net/towns/scotch-plains-slash-fanwood/sections/education/articles/cyber-attack-causes-disruption-of-scotch-plains-fanwood-schools

[45] To learn more and access products in this series, visit: https://www.k12six.org/protective-measures-series

[46] Developed by K-12 IT practitioners, for K-12 IT practitioners—and aligned to cybersecurity risk management best practices—the K12 SIX 'Essential Protections' series establishes baseline cybersecurity standards for U.S. school districts and provides guidance on their implementation. K12 SIX-recommended practices are designed to defend against the most common cyber threats facing school districts, including those recently identified by the Federal Bureau of Investigation (FBI) and the Cybersecurity & Infrastructure Security Agency (CISA). To learn more and access products in this series, visit: https://www.k12six.org/protective-measures-series

[47] Reber, Chris (November 12, 2020). "Thorpe raises cyber insurance." Times News Online. Available online at: https://www.tnonline.com/20201112/thorpe-raises-cyber-insurance/

[48] See, e.g., Blosfield, Elizabeth (March 2, 2022). "Education Providers Face Challenges With Growth in Cyber Threats, Insurance Costs." Insurance Journal. Available online at: https://www.insurancejournal.com/news/2022/03/02/656160.htm; Childers, Angela (July 12, 2021). "Schools hit with cyber price hikes." Business Insurance. Available online at: https://www.businessinsurance.com/article/20210712/NEWS06/912342944/Schools-hit-with-cyber-price-hikes; Toulas, Bill (January 22, 2022). "School District reports a 334% hike in cybersecurity insurance costs." Bleeping Computer. Available online at: https://www.bleepingcomputer.com/news/security/school-district-reports-a-334-percent-hike-in-cybersecurity-insurance-costs/; Schaffhauser, Dian (October 12, 2021). "The Changing Face of Cyber Insurance in K–12." THE Journal. Available online at: https://thejournal.com/articles/2021/10/12/the-changing-face-of-cyber-insurance-in-k12.aspx

[49] Consortium for School Networking (December 2021). "2021 State and Federal Cybersecurity Policy Trends: Insights for Education Technology Leaders & Policymakers." Available online at: https://emma-assets.s3.amazonaws.com/paqab/20bc4de8816d684fc9af37751b204c19/CoSN_2021_Cybersecurity_Legislation_Report_11_30_21__2_.pdf

[50] See, e.g., Sabin, Sam (October 12, 2021). "New K-12 cybersecurity law is just the first step." Politico. Available online at: https://www.politico.com/newsletters/weekly-cybersecurity/2021/10/12/new-k-12-cybersecurity-law-is-just-the-first-step-798142

[51] See, e.g., Lohrmann, Dan (November 14, 2021). "Dedicated State and Local Cyber Grants Are Finally Arriving." Government Technology. Available online at: https://www.govtech.com/blogs/lohrmann-on-cybersecurity/dedicated-state-and-local-cyber-grants-are-finally-arriving

[52] See, e.g., GAO (October 2021). "CRITICAL INFRASTRUCTURE PROTECTION: Education Should Take Additional Steps to Help Protect K-12 Schools from Cyber Threats (GAO-22-105024). Available online at: https://www.gao.gov/products/gao-22-105024

[53] "Introducing the K-12 Cyber Incident Map" (March 30, 2017) available online at: https://k12cybersecure.com/blog/introducing-the-k-12-cyber-incident-map/

[54] Information about the Verizon Data Breach Incident Report (DBIR) series can be found online at: https://enterprise.verizon.com/resources/reports/dbir/

[55] The Common Core of Data (CCD) is the U.S. Department of Education's primary database on public elementary and secondary education in the United States. The U.S. Department of Education's Fast Response Survey System (FRSS) was established to collect issue-oriented data—representative at the national level—quickly and with minimum response burden.

[56] The U.S. Census Bureau's Small Area Income and Poverty Estimates (SAIPE) program provides estimates of income and poverty for every state and county. SAIPE also provides estimates of the number of school-age children in poverty for all school districts.

[57] For more information on the K-12 Cyber Incident Map, the technology used to build it, and functionality, see "Introducing the K-12 Cyber Incident Map, Version 2." https://k12cybersecure.com/blog/introducing-the-k-12-cyber-incident-map-version-2/

Osseo Area Schools

Proposed Board of Education July-December 2024 Agenda/Calendar

	July	August	September	October	November	December
District Policy		• **Policy Committee Mtg** (8/20/24)		• **Policy Committee Mtg** (10/8/24)		• **Policy Committee Mtg** (12/10/24)
Op Over-sight	**Regular Meeting** (7/23/24) • Consent agenda (teacher contracts) • Gifts to the district • Electric bus contract (brief meeting to act on required business)	**Work Session** (8/20/24) • 2024-25 Strategic Priorities and Operational Plan 279Online Update • Board calendar review **Regular Mtg** (8/27/24) • Superintendent's Report • Non-public contracts for Student Services • BBF Update Presentation • Summer Programming Report Presentation • Contract approvals • Negotiation Strat Mtg (closed)	**Work Session** (9/10/24)) • Attendance boundary changes: overview, timeline and process • Repurpose site: communications and engagement plan • Board calendar review ~~Hold for Extra Work Session 9/17/24~~ cancelled **Regular Mtg** (9/24/24) • Introduction of Student Board Representatives • Superintendent's Report • Preliminary Levy (action item with presentation) • Preliminary FY 2024 Financial Report (presentation) • General Liability Insurance Renewal • Negotiation Strat Mtg (closed)	**Work Session** (10/8/24) • ELA Curriculum and Structured Literacy Review • Cyber Security **Regular Mtg** (10/22/24) • Brooklyn Middle Steam programming presentationStudent Board Representatives Report • Superintendent's Report • Contract ratifications • Lobbyist contract approval • Negotiation Strategies Meeting (closed session)	**Special Mtg – Election Canvassing** (11/12/24) followed by **Work Session** • Comprehensive Engagement and Civic Readiness (CECR), formerly World's Best Workforce, Results • LRFP Budget Parameters • LTFM Update **Regular Mtg** (11/29/24) • Indigenous programming presentation • Student Board Representatives Report • Superintendent's Report • FY24 Financial Audit Results presentation • Combined polling place resolution • Negotiation Strategies Meeting (closed session)	**Work Session (12/10/24)** • Legislative Platform • Enrollment Update • Math curriculum update **Regular Mtg** (12/17/24) • Student Board Representatives Report • Superintendent's Report • Legislative Platform • Final Levy/Truth in Taxation • Contract ratifications • Negotiation Strategies Meeting (closed session) • Combined polling place resolution
Board Gov./ Self Gov.		**Work Session** • Standing item: Board calendar review	**Work Session** • Standing item: Board calendar review (15 min) • Board PD Session or Extra Work session (9/17/24)	**Work Session** • Standing item: Board calendar review (15 min)	**Work Session** • Standing item: Board calendar review (15 min)	**Work Session** • Standing item: Board calendar review (15 min)
Sup Rela tions			Establish individual board member meetings process (frequency TBD)	Develop superintendent evaluation/goal setting process		
Public Engage-ment						

Updated 9/26/2024

Osseo Area Schools

DRAFT Proposed Board of Education January-June 2025 Agenda/Calendar

	January	February	March	April	May	June
District Policy			• Policy Committee Meeting (3/11/25))			• Policy Committee Meeting (6/10/25)
Op Over-sight	**Organizational Meeting** (1/7/25) • Swearing in of new board members • Election of board officers • Board compensation • Consent agenda (business, legal) • Committee and Joint Board representatives • Informational Items: Operating Protocols – Resolution and Agenda Setting followed by **Work Session** ~~• Monitoring Report: Strategic Direction D Initiatives~~ **Hold for Extra Work Session or PD** 1/14/25) • School Board 1-year through 3-year Governance Work Plan **Regular Mtg** (1/21/25) • Student Board Representatives Report • Contract ratifications • Negotiations Strategy Meeting (SM/closed session)	**Work Session** (2/11/25) LRFP Budget Update • FY 2025 Mid-Year Budget Update ~~• Address Disparities for BIPOC Students (Strategic Direction E)~~ **Regular Mtg** (2/25/25) • Student Board Representatives Report • FY25 Budget Adjustments • FY25 Capital Budget Approval • Contract ratifications • Negotiations Strategy Meeting (SM/closed session)	**Work Session** (3/11/25) • xxx **Regular Mtg** (3/18/25) • Student Board Representatives Report • Technology bid awards • E-rate bid awards • Contract ratifications • Negotiations Strategy Meeting (SM/closed session)	**Work Session** (4/8/25) ~~• Monitoring report C~~ • Attendance boundary update **Regular Mtg** (4/22/25) • Student Board Representatives Report • District Planning Advisory Council (DPAC) Recommendations • Insurance renewals • Contract ratifications • Negotiations Strategy Meeting (SM/closed session)	**Work Session** (5/6/25) • Supt. Student advisory group (Amy T invite (advisory group to speak at work session – priorities chosen for school year 24-25 and beyond) • Achievement & Integration budget review *School Board closed session following work session for purpose of supt. evaluation* **Regular Mtg** (5/20/25) • Retiree recognition • Student board rep recognition • ECMAC Recommendations • Termination of probationary teachers • Contract ratifications • Negotiations Strategy Meeting (SM/closed session)	**Work Session** (6/10/25) • 2025-26 Budget • Legislative Update (WS/IO)20- ~~• Monitoring Report A~~ ~~• Monitoring Report B~~ **Regular Mtg** (6/24/25) • 2025-26 Budget • 10-year LTFM Plan • Contract ratifications • Negotiations Strategy Meeting (closed session
Board Gov./ Self Gov.	• Election of board officers/annual meeting (AR)					
Sup Rela-tions	• Mid-year Sup evaluation check-in (SM/Closed session, informal)	• Supt. Report BIPoC Advisory Committee • Supt. Report: Partnerships-Community & Govt Agencies	Supt Report: SRO Advisory Committee		School board conduct superintendent evaluation; report out (summary) at July meeting (closed meeting, May	
Public Engage-ment	~~• Monitoring Report D: Family & Comm Eng. measurable outcome rubric (Vision Card) (WS & RM/IO)~~					