Agenda
Osseo Area Schools
School Board

Regular Business Meeting
Brooklyn Middle STEAM School - Media Center
7377 Noble Ave. N.
Brooklyn Park, MN 55443
Tuesday, October 7, 2025
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 School Board of Osseo Area Schools is being conducted in 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/about-us/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
   Thomas Brooks, Board Vice Chair
2. 6:05 p.m. Check in
   Dr. Kim Hiel, Superintendent
3. 6:10-6:30 p.m. Welcome and Instructional Leader Presentation 2
   Kim Monette, Principal, Brooklyn Middle STEAM School
4. 6:30-7:30 p.m. Student Stakeholder Survey 11
   Dr. Bryan Bass, Asst. Supt. of Equity & Achievement; Amy Tollefson, District Level Principal and Student School Board Representatives; Tom Watkins, Coord. of Data & Assessment; Paula Forbes & Robin Francis, Finding Human Institute
5. 7:30-8:00 p.m. Cyber Security 36
   Anthony Padrnos, Exec. Dir. of Technology; Gerald Edwards, Director of Information Systems & Security; Gutema Dube, Cyber Security Analyst
6. 8:00-8:15 p.m. Board Calendar Review 148
   Dr. Kim Hiel, Superintendent
7. 8:15 p.m. Adjournment
   Thomas Brooks, 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 "About Us > School Board."

Osseo Area Schools

Welcome

October 7, 2025

Osseo Area Schools

STRATEGIC PRIORITIES 2025-26

MISSION

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.

VISION

Unleash and enhance the brilliance of our scholars to thrive and change the world.

CORE VALUES

HONOR AND INTEGRITY
BELONGING
INCLUSION
INNOVATION AND EXCELLENCE
TRANSPARENCY
INTRINSIC VALUE

Continuous Improvement Magnifier

A Create safe, welcoming and inclusive learning environments that foster global curiosity, belonging, innovation, and engagement.

- **A1** Implement the conditions that respect and value each and every scholars' race, culture and identity.
- **A2** Ensure secure learning environments that promote access and opportunity for equitable, innovative learning experiences across all district sites.

B Build and nurture a culture of achievement by providing content rich, rigorous, equitable, and individualized pathways.

- **B1** Ensure and confirm each scholar has access to high quality core instruction and interventions across the system.
- **B2** Improve pathways for college and career readiness to unleash student agency.

C Promote inclusive participation of our communities and provide timely, relevant, and easily accessible communication.

- **C1** Standardize the use of communication tools for timely, accessible, accurate information.
- **C2** Foster inclusion for diverse community voices, engagement, and collaboration.

D Create a system of operational innovation, excellence, accountability, and sustainability.

- **D1** Refine district, department and site operation plans to serve as a tool to monitor the impact of continuous improvement efforts on student achievement.
- **D2** Ensure consistent system-wide implementation of evidence-based staff retention strategies.

How do our **continuous improvement** cycles and processes help address and eliminate disparities and inequities in achievement?

3 Cs to align work

CONSISTENCY

- → Our responsibilities
- → Our behavior
- → Understanding our biases
- → Understanding expectations

CONNECTION

- → Our relationships
- → Our roles
- → Our impact on others
- → Build trust

COHERENCE

- → The why
- → Our decisions
- → Our data
- → Weight on the system

Osseo Area Schools

MISSION

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.

VISION

Unleash and enhance the brilliance of our scholars to thrive and change the world.

CORE VALUES

HONOR AND INTEGRITY
BELONGING
INCLUSION
INNOVATION AND EXCELLENCE
TRANSPARENCY
INTRINSIC VALUE

S 5-26

B Build and nurture a culture of achievement by providing content rich, rigorous, equitable, and individualized pathways.

B1 Ensure and confirm each scholar has access to high quality core instruction and interventions across the system.

B2 Improve pathways for college and career readiness to unleash student agency.

s to align work

STENCY
esponsibilities
behavior
erstanding our biases
erstanding expectations

ECTION
elationships
oles
mpact on others
trust

RENCE
vhy
decisions
data
ht on the system

Osseo Area Schools

MISSION

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.

VISION

Unleash and enhance the brilliance of our scholars to thrive and change the world.

CORE VALUES

HONOR AND INTEGRITY
BELONGING
INCLUSION
INNOVATION AND EXCELLENCE
TRANSPARENCY
INTRINSIC VALUE

S

5-26

B Build and nurture a culture of achievement by providing content rich, rigorous, equitable, and individualized pathways.

B1 **Teacher Clarity** ensures equitable access to high quality Tier 1 instruction, and interventions across the school by establishing a **shared, explicit blueprint for success** for all students and using a John Hattie's **MetaX resource** for school-wide instructional adjustments.

B2 **Teacher Clarity** improves pathways for college and career readiness by making learning intentions, success criteria and relevancy explicit which shifts students from passive task-completion to **active self-assessors** who own their growth and learning, thus fundamentally unleashing **student agency.**

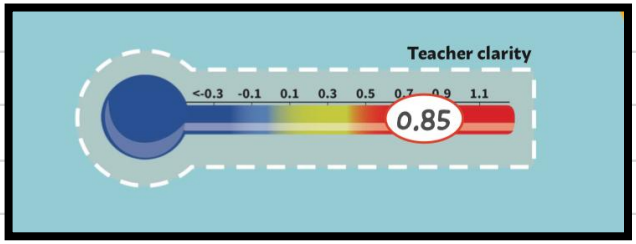
s to align work

STENCY
esponsibilities
behavior
rstanding our biases
rstanding expectations

ECTION
elationships
oles
mpact on others
trust

RENCE
vhy
decisions
data
ht on the system

BMS **Teacher Clarity** Journey



2022-2023

Monette & Havelak attend Visible Learning Conference. Introduce **Teacher Clarity** work in collab time with a focus on Learning Intentions and Success Criteria

2023-2024

Instructional Leaders attend Visible Learning Conference and ALL Staff begin deep dive into **Teacher Clarity** Work

2024-2025

Solidify Learning Intentions and Success Criteria and introduce Relevancy

2024-2025

Introduce work with Tier 2&3 Academic Vocabulary

Laser like focus on Explicit Instructional Teaching Strategies and implementing Teacher Clarity and Critical Reading Strategies

2025-2026

Train more teachers in Visible Learning (Summer 2026) to maximize teacher leaders and influencers

2026-2027

Why Visible Learning: Teacher Clarity?

- **Reason for Change:** A significant number of staff retirements, promotions to district leadership, and relocations created a critical need to **stabilize and strengthen** our instructional base.
- **Strategic Insight:** We recognized the urgency of building our **internal capacity** by developing a strong **instructional leadership team AND teacher leaders.**
- **Adopting High-Impact Teaching Strategies:** To ensure accelerated student growth, we sought out and committed to integrating **High Achieving Strategies and Instructional Practices** with the greatest proven impact on student learning.
- **Focus on Evidence-Based Training:** Our goal was to equip our incoming and current staff with a **unified, powerful toolkit** of Tier 1 instructional practices, leading us to deep engagement with the highly effective **Visible Learning** research by John Hattie's: Teacher Clarity work.

What is Visible Learning?

- A synthesis of over 1,200 meta-analyses on educational interventions, revealing that the most impactful factor for student achievement is making learning visible to students and teaching visible to teachers

- It emphasizes shifting focus from **what teachers *do* to the *impact* of what they do,** implementing evidence-based practices with the largest effect sizes, such as feedback, student expectations, and **teacher clarity**, to maximize learning outcomes across the district

- We decided to focus first on **TEACHER CLARITY**

BMS Common Vision

- **We believe in preparing students** by building **confidence, courage, and competence** — through leadership opportunities in their classrooms, school, and community.
- **We believe in providing opportunities and experiences** through **STEAM curriculum integration, project-based learning,** and **STEAM experiences** alongside professionals and experts.
- **We believe in creating a community of learners** by fostering a true **sense of belonging for each and every student.**
- **We believe in preparing all students for college and career readiness** through **AVID** and **STEAM partnerships** with the **University of Minnesota, Boston Scientific,** and other community partners.
- **We believe in Teacher Clarity** — grounded in John Hattie's *Visible Learning* research, ensuring that every student knows *what they are learning, why it matters, and how success is defined.*

Classroom and School Climate

“When we have high expectations and believe that ALL students will grow exceptionally, not simply making ‘normal’ progress. A core notion is that those who have high (or low) expectations tend to have this for all students.” (Hattie, Fisher, Frey, Almarode)

At BMS, WE EXPECT GREATNESS!

Classroom and School climate starts with expectations. We tend to get what we expect. When we expect greatness we are more likely to achieve it!

Osseo Area Schools

Student Stakeholder Survey Update

Tuesday, October 7, 2025

Dr. Bryan Bass, Amy Tollefson, Dr. Tom Watkins, Naomi Cooper-Grear, Aliya Jiwa, Cristian Vargas, Hikma Adam, Paula Forbes, and Robin Francis

Outcomes

Board members will:

- Learn about the ***purpose*** **and** ***history*** of the Student Stakeholder Survey
- Learn about the ***survey refinement process*** for collecting student input
- Learn about the ***role*** of the Student School Board Reps in the design and recommendation process
- Engage in ***discussion*** with Student School Board Reps

Osseo Area Schools

STRATEGIC PRIORITIES 2025-26

MISSION

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.

VISION

Unleash and enhance the brilliance of our scholars to thrive and change the world.

CORE VALUES

HONOR AND INTEGRITY
BELONGING
INCLUSION
INNOVATION AND EXCELLENCE
TRANSPARENCY
INTRINSIC VALUE

Continuous Improvement Magnifier

A Create safe, welcoming and inclusive learning environments that foster global curiosity, belonging, innovation, and engagement.

- **A1** Implement the conditions that respect and value each and every scholars' race, culture and identity.
- **A2** Ensure secure learning environments that promote access and opportunity for equitable, innovative learning experiences across all district sites.

B Build and nurture a culture of achievement by providing content rich, rigorous, equitable, and individualized pathways.

- **B1** Ensure and confirm each scholar has access to high quality core instruction and interventions across the system.
- **B2** Improve pathways for college and career readiness to unleash student agency.

C Promote inclusive participation of our communities and provide timely, relevant, and easily accessible communication.

- **C1** Standardize the use of communication tools for timely, accessible, accurate information.
- **C2** Foster inclusion for diverse community voices, engagement, and collaboration.

D Create a system of operational innovation, excellence, accountability, and sustainability.

- **D1** Refine district, department and site operation plans to serve as a tool to monitor the impact of continuous improvement efforts on student achievement.
- **D2** Ensure consistent system-wide implementation of evidence-based staff retention strategies.

How do our **continuous improvement** cycles and processes help address and eliminate disparities and inequities in achievement?

3 Cs to align work

CONSISTENCY

- → Our responsibilities
- → Our behavior
- → Understanding our biases
- → Understanding expectations

CONNECTION

- → Our relationships
- → Our roles
- → Our impact on others
- → Build trust

COHERENCE

- → The why
- → Our decisions
- → Our data
- → Weight on the system

Osseo Area Schools

STRATEGIC PRIORITIES 2025-26

MISSION

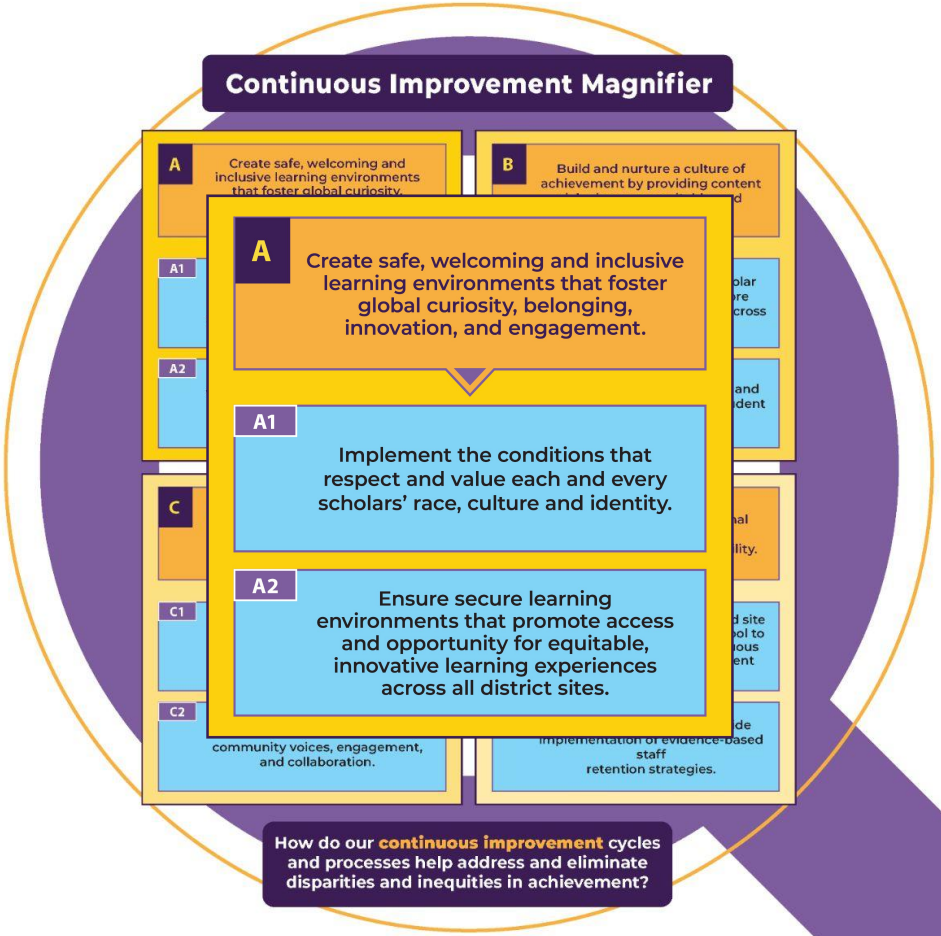
Our mission is to inspire and prepare each and every scholar with the confidence, courage and competence to achieve their dreams; contribute to community; and engage in a lifetime of learning.

VISION

Unleash and enhance the brilliance of our scholars to thrive and change the world.

CORE VALUES

HONOR AND INTEGRITY
BELONGING
INCLUSION
INNOVATION AND EXCELLENCE
TRANSPARENCY
INTRINSIC VALUE



3 Cs to align work

CONSISTENCY

- → Our responsibilities
- → Our behavior
- → Understanding our biases
- → Understanding expectations

CONNECTION

- → Our relationships
- → Our roles
- → Our impact on others
- → Build trust

COHERENCE

- → The why
- → Our decisions
- → Our data
- → Weight on the system

Osseo Area Schools

The concept of Holding Space

It means that we are willing to walk alongside another person in whatever journey they're on without judging them, making them feel inadequate, trying to fix them, or trying to impact the outcome. When we Hold Space for other people, we open our hearts, offer unconditional support, and let go of judgement and control.

— Heather Plett

Historical Overview

Student Stakeholder Survey

Purpose

- Measures progress on our Mission and Strategic Plan (including Vision Cards)
- Provides site leaders with feedback from students for school improvement
- Provided teachers with reports of student engagement in their class (2015-23)

2011-2014

2011-12 school year - “Mission Survey” in grades 5-12 measures *student perceptions of* ***Achieving Dreams***, ***Contributing to Community*** and engaging in ***Lifelong Learning***.

2013-14 - Mission Survey expanded to annual Student Stakeholder Survey for grades 3-12, scales added to measure ***Belonging***, ***Help at School***, ***Trusting Adults*****, and *Digital Learning***

2014-2015

2014-15 - The district adopts and adds scales of research-based questions for teacher-level student engagement reports in K-12: ***Engage, Illuminate, Manage, Relate, Stretch***

A subset of these questions are used at the school level to inform principal development and evaluation in grades 3-12: ***Classroom Learning***, ***Classroom Respect***, and ***Teaching***

2016-2025

2016-20 - Survey administered as in 2014-15

2020-21 - Survey not administered this year due to the pandemic

2021-23 - Survey administered as before the pandemic

2023-24 - Teacher-level questions, scales and reporting removed following ATPPS Steering Committee decision. School-level scales revised requiring a new baseline.

2024-25 - Survey administered as it was in 2023-24

Survey Refinement Process

Student Stakeholder Survey

Timeline

August - September

- Design process w/Student School Board Reps
- Selection of scholars

October - November

- Launch student listening sessions

November - December

- Analyze student feedback w/Student School Board Reps
- Create and prioritize recs.

January

- Scales revised w/student school board recs.

February - March

- Approve changes and launch revised survey

Focus Areas for Refinement

Safety – Strategic Direction A

Belonging & Inclusion – Core Values

Student Agency – Mission, Culture of Achievement

Future-Ready – Mission, Culture of Achievement

Partnership for 2025-26

Our district seeks to review and update survey language from scholars to ensure that all questions are student friendly

Process

Paula Forbes and Robin Francis from the Finding Human Institute LLC will host student listening sessions in the following areas:

- Safety
- Belonging & Inclusion
- Student Agency
- Future-Ready

Student Board Representatives

On September 23, 2025 Paula, Robin, Amy and Bryan met with the student representatives to frame the work and create powerful questions that will be asked of the following scholars:

- 4-5 (two listening sessions)
- 6-8 (three listening sessions)
- 9-12 (four listening sessions)

The format that will be used to collect information will be *The World Cafe*.

Sampling of Powerful Questions for each grade level

Grades 4-5

Safety

When do you feel safe at school and who helps you feel that way?

Belonging

What has a student or teacher done that helped you feel like you belong?

Inclusion

What could we do so that every student feels included in our school?

Grade 6-8

Safety

If you could change one thing about our school to make it safer, what would it be?

Belonging

When have you felt heard in spaces with students or adults at school?

Inclusion

What are some ways you have personally included others, or seen others include you?

Grades 9-12

Safety

What does feeling safe at school mean to you—physically, emotionally, and socially?

Belonging

Have you ever felt heard in spaces with people in power (like principals, teachers, or district leaders)? What difference did it make?

Inclusion

Imagine our school as a place where all students feel included—what would it look, sound, and feel like, and how could you help make it happen?

Synthesis Workshop and Survey

Following all of the listening session, we will reconvene with the Board representatives and leaders to synthesize the data and create a selection of survey questions.

The recommendations will be refined by the research team and incorporated into the survey.

The questions will be sent out to the entire student body.

The responses will be presented to school leaders and the board for analysis and action.

Pause & Process (Discussion)

- When you think about sharing your voice in this process, what would you like the end result to reflect?

- If the survey could help improve one part of your school experience — ***safety, belonging, student agency, or future ready*** — which would you pick and why?

Next Steps

Determine focus questions for student Agency and Future-Ready with Student School Board Reps

Launch listening sessions with scholars' grades 4-12

Questions?

Thank you!

Student Stakeholder Survey Scales and Questions

For each question, students could respond "Yes/Always", "Mostly Yes", "Maybe/Sometimes", "Mostly No", or "No/Never".

Scales and Questions
Achieve Dreams (grades 5-12)
1. At school I am learning to recognize my strengths.
2. I feel good about my future.
3. I have dreams for my future.
4. Someone at my school has helped me identify my dreams.
5. Someone at my school has helped me set goals for achieving my dreams.
Contribute to Community (grades 5-12)
6. I resolve conflicts without anyone getting hurt.
7. Students at my school from different races, ethnicities and cultures get along well together.
8. Students speak up to support other students if they are being disrespected or bullied
9. This year, I have helped to meet the needs of others through leadership, service, or some other way.
Lifelong Learning (grades 5-12)
10. Even when my work gets hard, I stick with it.
11. I manage my time well.
12. I plan ahead and make good choices.
13. If I can't figure something out on my own at school, I ask for help.
Belonging (grades 3-12)
14. At my school, teachers care about students.
15. I am comfortable sharing my thoughts and ideas at school.
16. I build friendships with other people.
17. I feel like I belong at school.
18. I feel respected at school.
Digital Learning (grades 3-12)
19. I feel safe and respected when interacting with other students online.
20. I have learned how to use technology in a safe and respectful way
21. I use technology to create products to show what I am learning
22. Technology helps me to work with my classmates.
23. When using technology at school, I get to create and discover new things.
Help (grades 3-12)
24. An adult at school has talked to me about how I am doing in my classes.
25. I have what I need to be successful at school.
26. If I have a problem, I have at least one adult at school that I can turn to.
27. If I have problems at school, the adults listen to me and help me.
Classroom Learning (grades 3-12)
28. During class, students avoid getting distracted by cell phones.
29. My race and culture are important and valued in what I am learning.
30. Things I learn in school are useful.
Trust (grades 3-12)
31. Adults in my school believe I can learn and will be successful.
32. Adults in my school trust me.
33. Adults in this school care about me.
34. Adults treat me with respect.
35. I can count on the adults at my school to help me learn and achieve.
36. The school rules are fair.

TO: Osseo Area Schools Board
FROM: Anthony Padrnos; Executive Director of Technology
Gerald Edwards; Director of Information Systems & Security
SUBJECT: Cybersecurity Update
DATE: October 7, 2025

Background

This annual update provides the Board with a comprehensive 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 and ensure service continuity. The objectives are to inform the Board of recent trends, emerging threats, legislative developments, and our strategic initiatives to enhance the district's cybersecurity posture.

K-12 Cybersecurity Landscape

The cybersecurity landscape for K-12 education has grown increasingly complex and challenging over the past year. Schools nationwide are facing a surge in sophisticated cyber threats, with malware such as SocGholish, NanoCore, and CoinMiner exploiting vulnerabilities through malvertisement and phishing campaigns. Attackers are strategically timing incidents to coincide with critical academic periods, such as exams and the start of the school year, amplifying operational disruption and ransom compliance risks. These attacks not only threaten digital assets but also disrupt essential services that schools provide to students, families, and the broader community. Legislative responses at the state level have intensified, with new laws focusing on centralized oversight, mandatory cyber insurance, workforce development, and improved incident reporting. Despite these efforts, many districts remain under-resourced, highlighting the need for ongoing investment, collaboration, and resilience planning to safeguard educational environments.

Current State of Cybersecurity in Osseo Area Schools

Osseo Area Schools has made significant strides in strengthening its cybersecurity posture, leveraging advanced monitoring and detection technologies across thousands of endpoints. Through partnerships with Red Canary and Microsoft Defender, the district processes billions of telemetry records annually, enabling continuous threat detection and rapid response to security alerts. Over the past year, dozens of confirmed threats were identified and addressed, with most detected through proactive analytics and expert investigation. The district is formalizing incident response plans and conducting tabletop exercises to ensure preparedness among IT staff and leadership. Service continuity planning has become a central focus, aiming to maintain critical operations, such as meal programs and emergency communications, even during cyber incidents. These efforts reflect a commitment to not only protecting digital assets but also ensuring the uninterrupted delivery of vital services to the school community.

Cybersecurity Initiatives

Osseo Area Schools continues to advance its cybersecurity initiatives through a strategic blend of training, monitoring, and response activities. Staff participate in regular phishing simulations and awareness campaigns, with training programs expanding to include custom modules for departments like HR, Enrollment, and Finance. The district is enhancing its use of Microsoft E5 security tools and developing internal playbooks to improve detection and escalation processes. Looking ahead, Osseo is exploring the implementation of a district-level Security Operations Center (SOC) to further strengthen its monitoring and incident response capabilities. Formal incident response plans are being drafted, and alignment with cyber insurance requirements is underway to ensure comprehensive coverage. These initiatives are designed to foster a culture of cyber awareness, integrate best-in-class security technologies, and build organizational resilience against evolving threats.

Conclusion

Osseo Area Schools continues to strengthen its cybersecurity posture through strategic investments in technology, training, and partnerships. The district is committed to proactive risk management, service continuity, and building resilience to protect students, staff, and the broader community. Ongoing legislative changes and evolving threats require sustained attention and adaptation. The Board's support remains critical as we advance our cybersecurity initiatives and safeguard our educational mission.

Att.

- Board Update Slides
- MS-ISAC K-12 Cybersecurity Assessment Report
- 2025 State Cybersecurity Legislation Report
- 2024 FBI Internet Crime Report

Osseo Area Schools
11200 93rd Ave. N
Maple Grove, MN 55369

763–391–7000
info@district279.org
OsseoSchools.org

Osseo Area Schools

Annual Cybersecurity Update

October 7, 2025

Anthony Padrnos; Ed.S., CETL
Gerald Edwards Sr.; CETL
Gutema Dube

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

Malware Threats

Dominant 2024 Malware:

QakBot and CoinMiner were the main malware threats in 2024, spreading via malspam and system vulnerabilities.

Shift in 2025 Malware Landscape

SocGholish became the leading malware in 2025, using fake browser updates and malicious ads for distribution.

Emerging Threats

New malware like NanoCore and ZPHP highlight the growing complexity of cyber risks in schools.

Attack Vectors

2024 Primary Attack Vectors

In 2024, malspam and combined methods like dropped malware and phishing emails were the leading infection vectors in schools.

Surge of Malvertisement in 2025

Malvertisement became the top infection vector in 2025, causing 63% of initial infections through malicious online ads.

Strategic Shift in Cyber Attacks

Cybercriminals targeted school browsing habits by exploiting seemingly safe web content, increasing malvertisement attacks.

Timing & Complexity

Strategic Timing of Attacks

Cyber attacks in 2025 are timed to critical academic periods like exams and school year start for maximum impact.

Increased Attack Sophistication

Threat actors now align attacks with school operational rhythms, showing advanced planning and sophistication.

Vulnerability During High Pressure

Schools are most vulnerable during exam weeks and maintenance windows, increasing ransom compliance risk.

Community Impact

Broader Community Impact

Cyber incidents in schools disrupt essential services affecting students, families, and the wider community.

Service Continuity Planning

Developing plans ensures critical services like meal programs and emergency communications continue during incidents.

Resilience Beyond Recovery

Focus shifts to comprehensive resilience planning recognizing schools as vital community infrastructure.

Legislative Conversation

- Centralized Oversight
- Cyber Insurance Requirements
- Workforce Investments
- Incident Report
- Data & Privacy Standards

FBI Cyber Crime Report

1. Ransomware remains the top threat
2. Most common school incidents are data breaches and phishing
3. Financial impact is rising
4. Business email compromise targeting school staff a growing concern

State of Cybersecurity in Osseo Area Schools

Background: Endpoint Collection

Custom range July 1, 2024 - June 30, 2025

13 billion+
telemetry records

Endpoint Footprint

Google Workspace, Microsoft Defender for Endpoint, and Microsoft Office 365 sensors are deployed on 6,460 endpoints.

Monitored endpoints include:
- 99% Windows
- 1% Unknown

Raw Telemetry

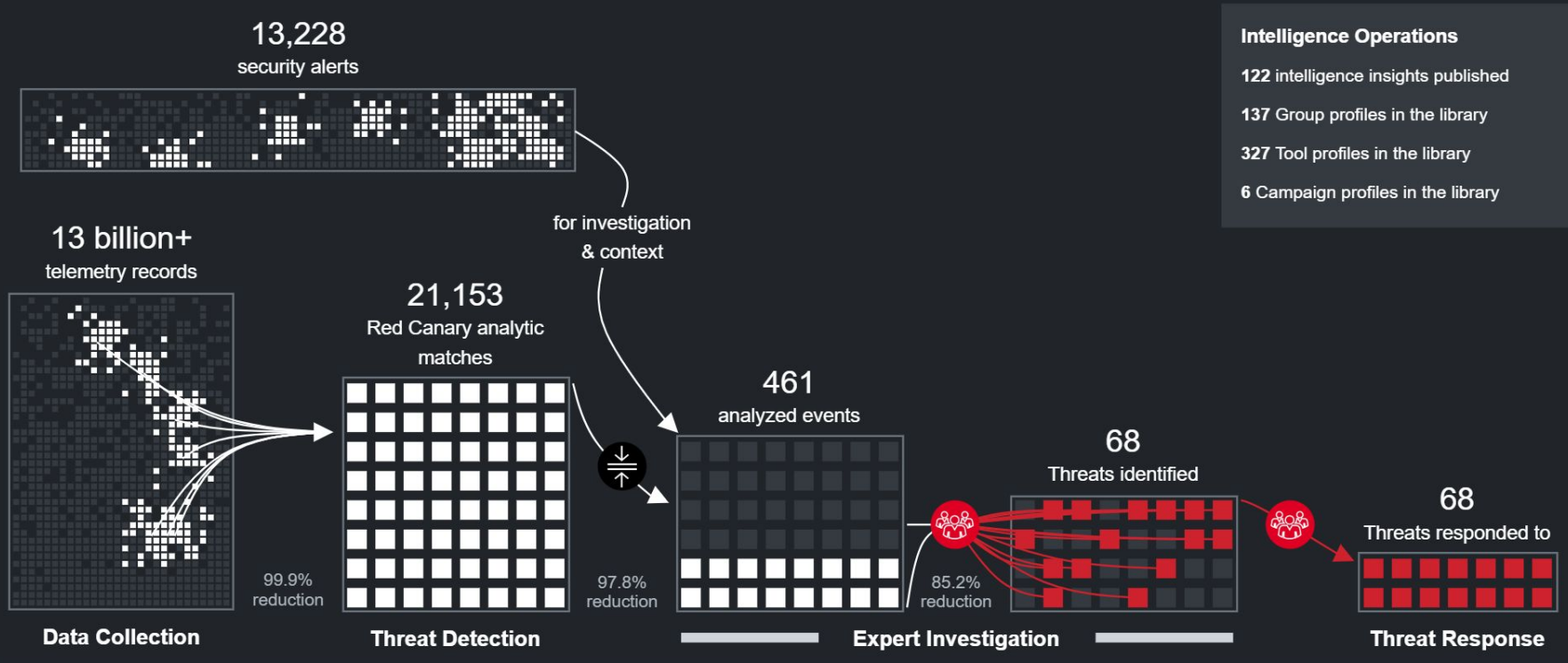
Key Takeaways

We processed 30.9 TB of telemetry from your endpoints, consisting of 13 billion+ telemetry records.

Processing this amount of data using a cloud SIEM would cost roughly $163,400 / year.

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

Custom range July 1, 2024 - June 30, 2025



11 products integrated
30.9 TB data ingested

5,075 detection analytics applied
591 threat hunts performed

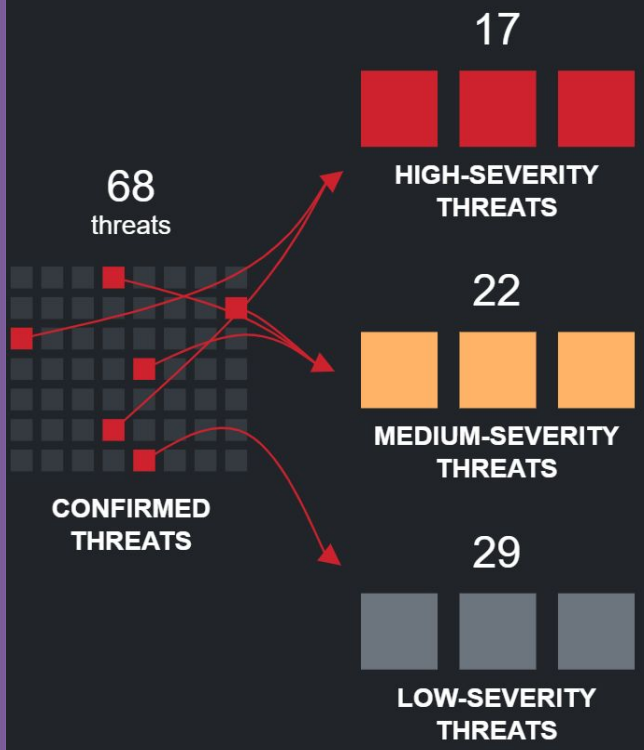
60 alerts associated with a Threat
13.2k alerts not associated with a Threat

17 high severity Threats
39 Red Canary unique Threats

0 remediations by Red Canary
790 playbook actions triggered

Background: Threats

Custom range July 1, 2024 - June 30, 2025



Key Takeaways

Red Canary's CIRT confirmed 39 medium and high severity threats:

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

Confirmed threats were identified in one way:

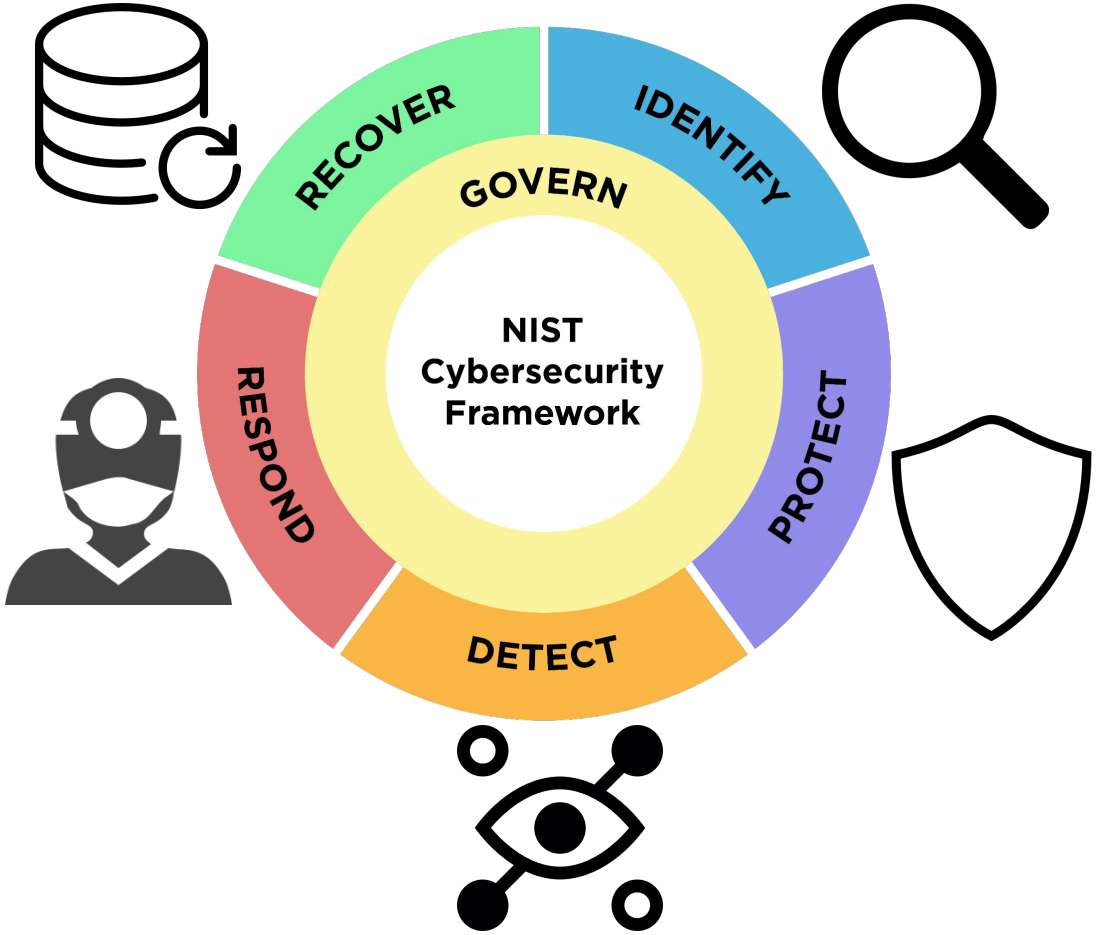
- 76% were identified by Red Canary's analytics

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

- 7 tactics (led by Command and Control and Defense Evasion)
- 12 techniques (led by Remote Desktop Software and Cloud Accounts)

Confirmed threats contained 79 annotations from the Red Canary CIRT that provided context and guidance to your response teams.

Cybersecurity Work in Osseo Area Schools


RECOVER
IDENTIFY
GOVERN
NIST
Cybersecurity
Framework
RESPOND
PROTECT
DETECT

Focus

Training

Monitoring

Response

Digital Security Training

We have a baseline

- Phishing simulations run using Microsoft Defender.
- General awareness training completed by staff.

We’re improving

- Expanding training to all employees, with custom modules for HR, Enrollment, and Finance.
- Establishing recurring phishing simulations and awareness campaigns.

We’re strategic

- Building a culture of cyber awareness across staff and students

Digital Security Monitoring

We have a baseline

- Red Canary monitors ~13B telemetry records annually.
- Microsoft Defender deployed on [6,400+ endpoints.]

We’re improving

- Expanding full use of Microsoft E5 security tools.
- Developing internal playbooks for detection & escalation.

We’re strategic

- Exploring Microsoft Sentinel to build a district-level Security Operations capability (SOC model).

Digital Security Response

We have a baseline

- Vendor (Red Canary) & Microsoft Defender XDR provides 24/7 threat alerting.
- Vulnerability assessments guide remediation.

We’re improving

- Drafting a formal Incident Response Plan.
- Planning tabletop exercises with IT and leadership.

We’re strategic

- Aligning with cyber insurance requirements.
- Building a clear, district-owned response framework.
- With budget alignment, enhance Microsoft Defender & Sentinel for district-level incident response capability.

Cybersecurity Growth Path: OAS

Baseline

- Red Canary actively used for 24/7 threat monitoring
- Microsoft Defender deployed district-wide
- Initial phishing simulations and awareness training conducted

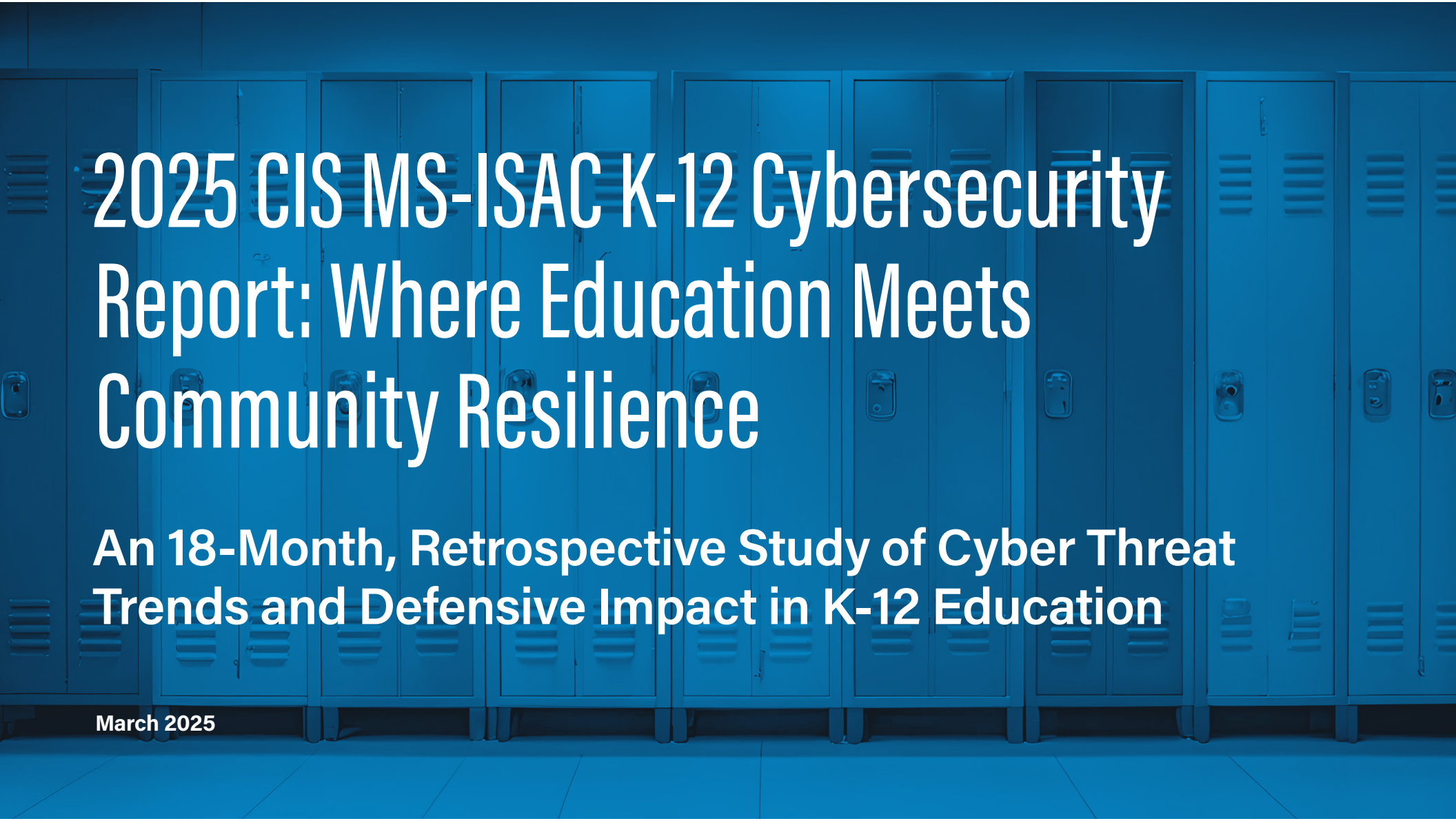
Continued Improvement

- Researching threat actor trends and staying ahead of evolving attacks
- Tailored training for HR, Finance, and Enrollment
- Enhancing the district Incident Response Plan with tabletop exercises

Strategic (Ongoing Focus)

- Strengthening integration of existing security tools
- Building a sustainable culture of cybersecurity awareness for staff and students

Questions?



2025 CIS MS-ISAC K-12 Cybersecurity Report: Where Education Meets Community Resilience

An 18-Month, Retrospective Study of Cyber Threat Trends and Defensive Impact in K-12 Education

March 2025

CIS Center for Internet Security®

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

Produced by Center for Internet Security, in partnership with Consortium for School Networking.

© 2025 - Center for Internet Security, Inc.

Contents

Where was content sourced for this report?

The following information details the results of an 18-month study covering July 2023 - December 2024. Data for this report was collected from multiple sources, including more than 4,600 K-12 entities in the MS-ISAC. Sources include data collected from respondents to the 2023 and 2024 Nationwide Cybersecurity Review (NCSR), MS-ISAC member feedback, services data, direct reporting data from the CIS Security Operations Center (SOC), data from CIS Cyber Incident Response Team (CIRT) engagements, and threat data and associated analysis by the CIS Cyber Threat Intelligence (CTI) Team.

Who We Are

Every day, the Center for Internet Security, Inc.® (CIS) and Multi-State Information Sharing and Analysis Center® (MS-ISAC®) work alongside K-12 schools in their mission to protect not just computer systems but communities. We understand that when a cyber attack hits a school, it affects far more than just emails and databases — it impacts childrens' access to meals, parents' ability to work, and even community life itself.

CIS® Center for Internet Security®

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

Supporting Partner

CoSN Leading Education Innovation

CoSN, the world-class professional association for K-12 EdTech leaders, stands at the forefront of education innovation. We are driven by a mission to equip current and aspiring K-12 education technology leaders, their teams, and school districts with the community, knowledge, and professional development they need to cultivate engaging learning environments. Our vision is rooted in a future where every learner reaches their unique potential, guided by our community.

CoSN represents over 2050 school districts reaching over 11 million students. Our state presence is expanding with 33 CoSN Chapters in 34 states who function at the grassroots level to further effect change and continues to grow as a powerful and influential voice in K-12 education.

Executive Summary

In a small rural district last winter, a ransomware attack struck during midterm exams. As systems went dark, the impact cascaded far beyond the school's digital infrastructure. The cafeteria staff, unable to access their electronic systems, scrambled to feed hundreds of students who depended on school meals. Parents, many working hourly jobs, suddenly needed to find childcare when classes were canceled. The graduating senior class worried about college application deadlines as their transcripts suddenly became inaccessible.

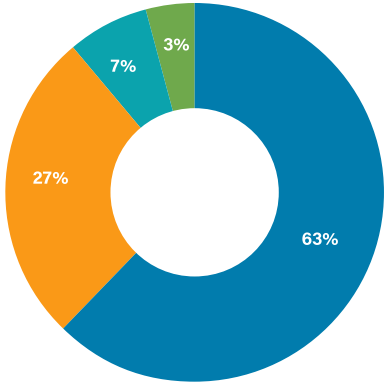
The above scene is an all too common one that has played out in schools across America year after year. Cyber attacks on educational institutions create ripples that affect entire communities. Our analysis of 18 months of data from more than 5,000 K-12 organizations shows that cyber threat actors appear to be increasingly targeting schools during critical periods like exams, times when the pressure to maintain operations makes schools far more vulnerable to ransom demands.

Definition

K-12 organization: Public schools and districts educating students from kindergarten to 12th grade.

Top Malware Infection Vectors

- Malvertisement
- Multiple
- Dropped
- Malspam



The Scale of Impact:

- **82% of K-12 organizations experienced cyber incidents**
- **Nearly 14,000 security events observed**
- **Over 9,300 confirmed incidents**
- **Cyber threat actors target human behavior 45% more often than technical vulnerabilities**

What makes this report's findings particularly troubling goes beyond the number of attacks and confirmed incidents. Rather, we see a significant increase in threat actors' sophistication and timing. We all know that schools serve as essential community infrastructure, and it appears threat actors have also begun to more heavily exploit this fact, as schools provide not just education but vital services:

- Nutritional support through breakfast and lunch programs
- Safe spaces for children of working parents
- Mental health and counseling services
- Special education and developmental support
- Community gathering spaces and resources

When cyber attacks disrupt these services, the effects ripple throughout the community. A parent missing work to care for a child during a school closure creates economic impact. A student missing meals due to cafeteria system outages affects their health and ability to learn. The loss of access to counseling services during critical times can have lasting effects on student well-being.

This report examines how K-12 organizations are responding to these challenges through collaboration, preparation, and a deep understanding that cybersecurity in education is fundamentally about protecting people, not just technology.

Lessons Learned: The Human Cost of Cyber Incidents

When a ransomware attack struck a district during midterm exams in the fall 2024 semester, it revealed a truth about school cybersecurity: these incidents affect far more than just technology. With systems inaccessible, students lost access to meals, parents were forced to arrange childcare, and graduating seniors likely worried about college application deadlines. This scenario, and countless others like it, illustrates what protecting schools from cyber attacks really means — it means protecting communities.

The Human Element: Primary Target

Analysis of incident data reveals a stark reality: cyber threat actors (CTAs) target human behavior exponentially more than any other attack vector. Our services blocked more than 1 billion connection attempts to malvertisement domains and 320 million connection attempts to phishing domains.

Key Findings:

Human-targeted threats exceeded other techniques by 45%

82% of reporting K-12 schools experienced cyber threat impacts

Over 9,300 confirmed incidents

Strategic Timing of Attacks

CIS Cyber Incident Response Team (CIRT) data combined with our security monitoring suggests that CTAs may increase attacks during specific times of the school year. Threat actors appear to ramp up the intensity of their attacks during the beginning of the school year, the mid-term period, and the very end into the summer. These periods could overlap with critical functions such as new staff and student acclimation, mid-term and end-of-year exam weeks, and summer network maintenance periods. Schools face maximum pressure to restore services during critical times, particularly exam periods. The timing of attacks may demonstrate increasing sophistication of cybercriminals and a move toward strategic targeting K-12 organizations during the academic calendar's pressure points.

Beyond the Digital Impact

Not all cyber incidents are created the same, and incidents that lead to schools needing to temporarily shut down impact more than simply the ability to access files.

When cyber incidents force schools to close or limit operations, vital services disappear. The impact extends far beyond missed classes, threatening the basic support systems many families rely on.

Today's K-12 schools serve as more than a place where students prepare for their futures; K-12 schools are essential community infrastructure, enhancing the community by providing:

- Critical nutrition through meal programs.
- Safe spaces for student development.
- Special education and support services.
- Community gathering spaces.
- Extra-curricular activities.
- An increased sense of community.

Collaborative Response Makes a Difference

Schools that engage with the MS-ISAC's no-cost incident response services gain crucial support during cyber incidents. While many incidents go unreported due to a variety of factors (including cyber insurance stipulations and requirements), CIS CIRT data from incidents over the past 18 months indicates that early engagement and preparation significantly improve outcomes.

The K-12 Threat Landscape: An 18-Month Assessment of Risk and Impact

Our comprehensive analysis spanning July 2023 through December 2024 reveals that cyber attacks against schools appear to show tactical patterns. During examination periods across various academic terms, there is a heightened level of threat actor activity. These periods are crucial as they exert significant pressure on schools to sustain their operations amid potential security threats. This extended assessment period provides valuable insights into how attacks evolve across multiple academic cycles.

Patterns of Strategic Targeting

Cyber attacks against schools appear to show tactical patterns. Cyber threat actor activity appears to increase in intensity in relation to specific time periods of the school year, namely during examination periods, critical times during the school year when maintaining day-to-day operations is paramount. This pattern was observed across multiple academic terms. During these high-stakes periods, schools face a seemingly impossible choice: pay a ransom to restore services quickly or potentially compromise students' academic futures.

When a ransomware attack struck during midterm examinations, it revealed how deeply intertwined school technology has become with student success. Teachers lost access to testing materials and student records. Special education services, which rely heavily on detailed digital records and individualized education plans, faced significant disruption.

Impact derived from over 1 trillion logs over 18 months

82% of reporting K-12 schools experienced cyber threat impacts

14,000 Nearly 14,000 security events observed

9,300 Over 9,300 confirmed incidents

The Evolution of Attack Methods

Our analysis shows that attacks targeting human behavior — particularly those through malvertising — exceeded other attack vectors by at least 45%. The trend toward attacks that target human vulnerabilities highlights the adaptability of threat actors, who are now exploiting the inherently supportive and trusting characteristics of educational settings. Teachers, administrators, and support staff, whose primary focus is helping students succeed, now find themselves on the front lines of cybersecurity defense.

How Cyber Threat Actors Exploit Humans in K-12 Settings

- Human-targeted threats exceed technical exploits by 45%
- Malvertisement leads all attack methods
- 66% of schools with endpoint protection affected

Community-Wide Disruption

Modern K-12 schools have evolved into essential community infrastructure, providing vital services that extend far beyond traditional education. When cyber attacks force schools to limit or temporarily cease operations, they don't just interrupt learning — the attack destabilizes the routine of community life itself.

Consider school meal programs, which serve as a critical source of daily nutrition for millions of students. When payment and verification systems go down, schools must choose between turning away hungry students or finding alternative ways to provide meals, all while having the same requirements of tracking the number of students who came through the line. Similarly, when special education programs and counseling services lose access to digital records and communication systems, our most vulnerable students face immediate challenges.

The economic impact ripples throughout the community as parents miss work to care for children who cannot attend school. This disruption particularly affects communities where the school system forms the backbone and routine structure of daily economic activity. A cyber attack on a school doesn't just impact education — it has an outsized effect on the stability and well-being of entire communities.

Collaborative Response: Building K-12 Cyber Resilience Through Partnership

The complexity and impact of cyber threats to K-12 organizations demands a response that extends beyond any single school or district. Our analysis reveals that the most resilient schools embrace a collaborative approach, leveraging partnerships and shared resources to protect their communities.

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

The Power of Proactive Partnership

MS-ISAC membership provides K-12 organizations with crucial support before, during, and after cyber incidents. This no-cost partnership provides schools with access to incident response services, cybersecurity advisory services, threat intelligence, and a network of cybersecurity experts who understand the unique challenges of educational environments.

Consider how these partnerships manifest in practice:

> When schools actively engage with the MS-ISAC and take full advantage of the no-cost and cost-effective resources exclusively available to them as members, they effectively add millions of dollars to their overstretched cybersecurity budgets, getting industry-leading cybersecurity solutions at a fraction of the commercial cost, and in many cases, completely free.

And for K-12 organizations that take the **Nationwide Cybersecurity Review (NCSR) assessment**, their cyber maturity increases by an average of 26%, enabling them to prioritize their limited resources while building defenses that account for both technical and human elements of security.

> Custom threat intelligence derived from within the K-12 sector of membership and broader MS-ISAC community leads to the highest and most impactful detections.
>
> 72% of all Endpoint Detection and Response (EDR) detections and 87% of all EDR incidents were caught from intelligence gathered from our internal investigations and analysis and deployed into the CIS Endpoint Security Services (ESS) environment.

Membership Benefits:

- Access to no-cost incident response services
- Real-time threat intelligence sharing
- Professional development opportunities
- Community-driven best practices
- ...and more.

Integrating Leadership and Technology

For the second year in a row, the Center for Internet Security is proud to see the MS-ISAC and Consortium for School Networking (CoSN) come together and partner on this report, dovetailing our separate missions to strengthen and empower K-12 educational leaders to create a comprehensive approach to school cybersecurity. This collaboration addresses key areas including:

Professional Development	Build capacity among teachers and staff to enable them to recognize and respond to cyber threats while maintaining focus on their primary educational mission.
Resource Optimization	Schools can and should take advantage of no-cost and cost-effective resources and collaborative solutions to help their cybersecurity budgets go further.
Encourage Opportunity in Security	Foster opportunities for smaller and under-resourced districts to access robust cybersecurity solutions, increasing their cyber maturity and helping them better defend against cyber attacks.
Risk Management	Take full advantage of expert-maintained cybersecurity best practices like the CIS Critical Security Controls®. The CIS Controls® balance security needs with educational accessibility, allowing K-12 organizations to apply controls in a manner that best addresses the challenges of their organization's unique environment.

Opportunities for Creating Resilient Communities

The most effective defense strategies recognize that school cybersecurity extends beyond protecting digital assets; it's about preserving the educational and social infrastructure that communities depend on.

This understanding drives the development of:

Response Networks

Schools can build connections with community organizations that can help maintain essential services during cyber incidents.

Communication Channels

K-12 organizations should establish clear protocols for keeping families and community members informed during security events.

Service Continuity

Schools should develop and regularly audit service continuity plans to maintain critical community services, especially for vulnerable populations, even when digital systems are compromised.

Recommendations: Protecting Schools, Preserving Communities

In developing cybersecurity recommendations for K-12 organizations, we understand that we must fundamentally shift how we think about the human element in cybersecurity. Our analysis shows that the most successful approaches treat people not as vulnerabilities to be managed, but rather, as powerful assets to be empowered.

Empowering the Human Element

Our research shows that K-12 organizations can achieve significantly better security outcomes when they instead foster an environment where every individual understands their vital role in protecting their school community.

While cybersecurity measures often focus on the technical aspects of securing the environment, integrating a human-first approach to security mirrors what K-12 organizations are already doing to address types of threats such as tornadoes or fires.

Creating a Culture of Cyber Empowerment

K-12 organizations should develop environments where everyone who accesses the network — from administrators to substitute teachers — feels they are a crucial part of the security team. What this means in practice is K-12 organizations should strive to:

- Build a shared understanding that every individual plays an active role in protecting students, families, and community services.
- Recognize and celebrate when staff members identify and report potential security concerns.
- Create open dialogue between IT security teams and educational staff to better understand each other's needs and challenges.
- Ensure all members of the school community understand how their actions directly contribute to protecting vital services.

Increasing Cyber Maturity Through Frameworks

The CIS Critical Security Controls (CIS Controls) are a prescriptive, prioritized, and simplified set of best practices that you can use to strengthen your cybersecurity posture. Today, thousands of cybersecurity practitioners from around the world use the CIS Controls and/or contribute to their development via a community consensus process.

> The traditional view of humans as the "weakest link" in cybersecurity has created a self-fulfilling prophecy in many organizations. When we consistently tell people they are a liability, they often unconsciously fulfill that role.

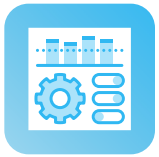
Moving Beyond Traditional Awareness

While security awareness training has its place, it should be viewed as just one small part of a larger cultural transformation. K-12 organizations should focus their efforts to:

- Develop collaborative relationships between IT security teams and educational staff, where both groups work together to find solutions that protect both security and educational needs.
- Create clear, accessible channels for staff to report concerns without fear of judgment or reprisal.
- Provide regular feedback to staff about how their vigilance and actions have helped protect the school community.
- Ensure leadership actively demonstrates that security is a shared responsibility, not just an IT concern.

Technical Framework Development

When technical controls complement and support human empowerment, rather than restrict and frustrate, organizations build stronger security. K-12 organizations should implement technology solutions that protect both their community and their mission.



Essential Security Controls

Security technology should enable and protect educational activities while remaining as frictionless as possible to users. Key implementations include:

- Multi-factor authentication designed with teacher workflows in mind, understanding that educators often need quick access while moving between classrooms or helping students.
- Backup systems that automatically protect critical data while allowing teachers to focus on teaching rather than manual backup procedures.
- Network design that protects sensitive information while ensuring teachers and staff can efficiently access the resources they need.
- Endpoint protection that focuses on preventing threats without creating barriers to educational software and resources.

Service Continuity Planning

Technical planning should prioritize maintaining essential community services during cyber incidents. Every organization is different, so the following recommendations are representative rather than prescriptive:

- Work with cafeteria staff to develop systems that keep meal programs running even if networks are compromised.
- Collaborate with teachers to create accessible backup copies of critical student records.
- Design emergency communication systems that staff can easily use during incidents.
- Maintain simple, paper-based backup procedures that staff can confidently implement when needed.

Strengthening Through Partnership

Partnerships multiply the effectiveness of both human and technical security measures. When organizations work together, they create networks of support that enhance everyone's resilience.

MS-ISAC Collaboration

MS-ISAC membership provides more than just technical tools — members establish connections that empower them. With a notification time 92% faster, on average, than most other MSSPs, the MS-ISAC delivers unparalleled value to members. Additionally, MS-ISAC members can:

- Access immediate support during incidents from cybersecurity and incident response experts who understand K-12 environments.
- Share insights and experiences with peer organizations facing similar challenges.
- Implement security monitoring that supplements local expertise.
- Build relationships with the broader K-12 cybersecurity community and other local government entities before crises occur.

Professional Growth

Professional development should focus on building confidence in addition to capability:

- Engage with CoSN to develop both technical skills and educational leadership.
- Practice incident response through collaborative tabletop exercises that build team confidence.
- Create opportunities for staff to feel heard and invite them to share their security experiences and insights.
- Identify and support staff members who show interest in becoming security advocates.

Fostering Community Resilience

Strong communities can help schools weather cyber incidents, but it is not automatic. K-12 schools must intentionally strengthen these relationships. Building these relationships requires:

Communication Development

Create communication strategies that:

- Establish trusted channels for sharing information with families during incidents.
- Build relationships with local media to ensure accurate, helpful coverage of your organization — whether your team just won the state tournament or your operations have been impacted by a cyber incident.
- Prepare clear, accessible templates for various types of incidents and implement these templates into your tabletop exercises to get real-world experience and gain confidence.
- Maintain strong connections with community partners who can provide support to your K-12 organization in the event of a cyber incident.

Service Protection

When a cyber attack impacts your ability to provide services — education, meals, activities, transportation — the fallout can be enormous. Prioritize protecting these essential services through active community engagement:

- Work with staff to identify the most critical services your school provides.
- Develop practical alternatives for maintaining these services with minimal disruption during incidents.
- Build partnerships with community organizations who can provide backup support.
- Create clear guidelines for service continuity that empower staff to make decisions.

Conclusion: Building Resilient Educational Communities Together

The challenges facing K-12 organizations and their cybersecurity extend far beyond protecting data and devices. When cyber incidents strike schools, they threaten the essential services that bind communities together. Our 18-month analysis reveals that schools serve as crucial community infrastructure, providing nutrition, safety, support services, and educational opportunities that families depend on every day.

Traditional approaches to cybersecurity have often treated humans as a weakness to be mitigated through training and restrictions. Thankfully, cybersecurity experts are realizing a new, more human-empowering approach is needed. The most resilient organizations take this fundamentally different approach. They recognize that their people — from teachers and administrators to support staff and technical teams — represent their greatest security asset when effectively empowered and supported.

This seismic shift from viewing people as liabilities to seeing them as essential defenders transforms how organizations approach security. When staff members feel valued and understand their crucial role in protecting their school community, they are more likely to become active participants in security rather than passive recipients of compliance-focused training. They develop the confidence to identify threats, the knowledge to respond effectively, and the understanding that their actions directly protect students, families, and essential services that extend far beyond the classroom.

The technical controls and partnerships we've discussed can make a significant difference,, and they function best when implemented in service of this human-centered approach. Multi-factor authentication, backup systems, and monitoring tools should support educational missions rather than impede them.

When K-12 organizations partner with organizations like the MS-ISAC and CoSN, they build capability and confidence alongside technical expertise.

The future is bright, and the path is well-lit, but the journey requires continued, intentional commitment to:

- Understanding schools as essential community infrastructure that provides vital services beyond education.
- Empowering every individual who accesses school networks to become an active defender of their community.
- Implementing technical controls that protect services while supporting educational missions.
- Building partnerships that enhance both human and technical capabilities.
- Creating resilient communities that can maintain essential services even during cyber incidents.

As we look to the future, the cybersecurity challenges facing K-12 organizations will undoubtedly evolve, but so will you. By fostering environments where every individual feels empowered to protect their school community, implementing supportive technical controls, and building strong partnerships, your organization can develop the resilience needed to face these challenges while continuing to serve your community.

Key Takeaways:

- **Schools are essential community infrastructure.**
- **Empowered humans are the strongest line of defense.**
- **Technical controls should support educational missions.**
- **Partnerships multiply organizational capabilities.**
- **Community resilience depends on maintaining essential services.**

Appendices

Appendix A: Understanding MS-ISAC Services for K-12 Organizations

The Multi-State Information Sharing and Analysis Center (MS-ISAC) provides:

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		✓

Appendices

Appendix A: Understanding MS-ISAC Services for K-12 Organizations (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		✓

Appendix B: Building Your Security Program

This section provides a scalable framework for establishing and maintaining an effective K-12 security program that empowers your educational community.

Program Elements	
Leadership Engagement	• Establish security as a school-wide priority • Champion active support for security initiatives • Allocate resources effectively
Community Integration	• Identify essential services your school provides • Map dependencies between services • Create service continuity plans
Technical Implementation	• Deploy fundamental security controls • Establish monitoring capabilities • Maintain backup systems
Partnership Development	• Engage with security organizations • Build local support networks • Share experiences with peer institutions

Appendix C: Resource Guide

Take advantage of the resources available to your organization. These resources have been developed by cybersecurity and threat intelligence experts and are maintained by dedicated teams of security professionals around the country and around the world.

Resource	
Incident Response Plan Template	Access Incident Response Plan Template
CIS Critical Security Controls®	https://www.cisecurity.org/controls
CIS Benchmarks®	https://www.cisecurity.org/cis-benchmarks
CIS Hardened Images®	https://www.cisecurity.org/cis-hardened-images

Appendix D: Glossary of Terms

This glossary provides clear, non-technical explanations of key concepts referenced throughout the report.

Glossary

Incident Response	The organized approach to addressing and managing the aftermath of a security breach or cyber attack.
Malspam	Email-based attacks wherein emails contain attachments or links that contain or deliver malicious software (malware).
Malvertisement	An attack tactic that uses internet advertisement space maliciously to spread malware and compromise systems.
Multi-factor Authentication (MFA)	A security method requiring users to provide two or more verification factors to gain access to a resource.
Ransomware	Malicious software that encrypts files, making them inaccessible until a ransom is paid.
Service Continuity	The capability of an organization to continue delivery of essential services at acceptable levels following a disruptive incident.

Appendix E: Nationwide Cybersecurity Review Results

2024 Nationwide Cybersecurity Review (NCSR)

The 2024 Nationwide Cybersecurity Review (NCSR) assessment is available to complete from October 2024 through February 2025. The below data reflects NCSR assessment submissions between October 2024 and December 2024.

286 K-12 school districts completed the NCSR assessment during this timeframe.

Here are aggregate data findings for the K-12 participants during this timeframe, as well as comparisons to historical data.

Top 5 Security Concerns

Lack of Sufficient Funding	**a.** 86% of K-12 participants selected in the 2024 NCSR **b.** 82% of K-12 participants selected in the 2023 NCSR
Increasing Sophistication of Threats	**a.** 61% of K-12 participants selected in the 2024 NCSR **b.** 61% of K-12 participants selected in the 2023 NCSR
Lack of Documented Processes	**a.** 52% of K-12 participants selected in the 2024 NCSR **b.** 53% of K-12 participants selected in the 2023 NCSR
Lack of a Cybersecurity Strategy	**a.** 37% of K-12 participants selected in the 2024 NCSR **b.** 38% of K-12 participants selected in the 2023 NCSR
Inadequate Availability of Cybersecurity Professionals	**a.** 32% of K-12 participants selected in the 2024 NCSR **b.** 37% of K-12 participants selected in the 2023 NCSR

K-12 School District Staffing

2024 86% of K-12 school districts stated they have less than 5 employees with security related duties.

2023 89% of K-12 respondents in the 2023 NCSR cycle stated they have less than 5 employees with security related duties.

K-12 Overall Maturity Scoring

2024 The overall average maturity score of K-12 NCSR participants was 3.76 on the NCSR's 1 through 7 scoring scale.

2023 This was an improvement compared to the 2023 NCSR cycle's average maturity score of 3.45

- The 2023 cycle average fell below the score of other local level sectors, such as public utilities, health services, and election offices.

K-12 School Districts & Security Framework Usage

2024 77% of K-12 school districts stated they use a security framework, such as the CIS Controls or the NIST Cybersecurity Framework (CSF).

- K-12 school districts that use a security framework scored 26% higher, on average, compared to those not using a framework.

2023 73% of K-12 respondents stating they use a framework during the 2023 NCSR cycle. K-12 schools using a framework scored 52% higher at that time.

K-12 High-Performing Areas

NIST Cybersecurity Framework (CSF) Categories:

- Protect: Identity Management & Access Control
- Respond: Mitigation
- Protect: Awareness and Training
- Detect: Security Continuous Monitoring
- Respond: Analysis

2023 The top three categories were the same compared to the 2023 NCSR cycle. The two changes within the top five scoring categories were the "Detect: Security Continuous Monitoring" category entering the top five, as well as the "Respond: Analysis" category entering the top five.

Specific Activity Areas:

- Having an inventory of physical devices and systems
- Managing and verifying identities/credentials for authorized users
- Managing remote access

K-12 Lower-Performing Areas

NIST Cybersecurity Framework (CSF) Categories:

- Identify: Risk Management Strategy
- Protect: Protective Technologies
- Detect: Anomalies & Events
- Recover: Improvements
- Recover: Communications

2023 The two changes within bottom five scoring categories were the "Recover: Improvements" category and the "Recover: Communications" category entering the bottom five.

Specific Activity Areas:

- Protecting and restricting use of removable media
- Detecting unauthorized mobile code
- Establishing and managing organizational risk tolerance
- Usage of integrity checking mechanisms to verify software integrity
- Aggregating and correlating event data from multiple sources and sensors
- Separating the development and testing environment(s) from the production environment

K-12 Lower-Performing NCSR Areas Aligned to CIS Controls

Note: The below details are more granular than the information earlier in this document, as it views specific NIST Cybersecurity Framework (NSF) subcategory activities aligned to the CIS Controls and applicable Control Safeguards.

NIST CSF Category	CIS Critical Security Control	Recommended Actions
Protect: 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 • Standardize Time Synchronization • Collect Command-Line Audit Logs • Conduct Audit Log Reviews
	CIS Control 10: Malware Defenses	• Disable Autorun and Autoplay for Removable Media
Recover: Communications	**CIS Control 17:** Incident Response Management	• Establish and Maintain Contact Information for Reporting Security Incidents • Define Mechanisms for Communicating During Incident Response

For a look at the previous year's NCSR data, see 2023 Nationwide Cybersecurity Review: https://learn.cisecurity.org/NCSR-2023-Summary-Report .

Appendix F: CTI Team Writeup with Data

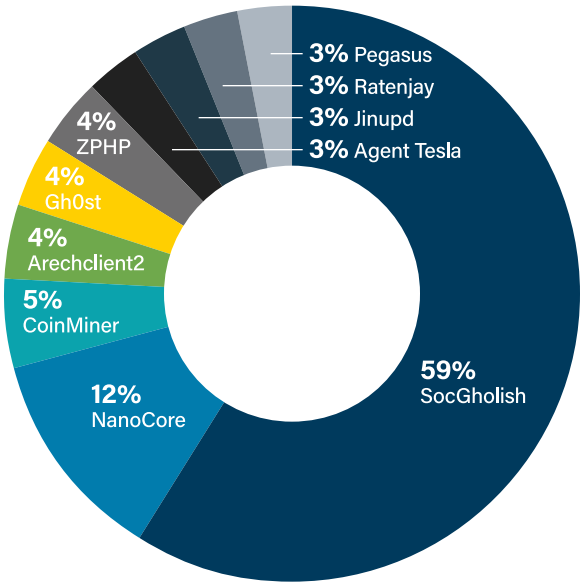
Top 10 Malware Affecting K-12 Schools

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 July 2023 through December 2024, SocGholish was the top malware affecting K-12 entities, making up 60% of the top 10 malware. This contrasts with the previous year where QakBot, a modular banking trojan, posed the most significant threat to K-12 entities. The year to year change is due to the end of QakBot's campaign and the beginning of a large scale SocGholish malware campaign. The second and third most prevalent malware were NanoCore and CoinMiner. The top 10 malware had a 50% change compared to the previous K-12 report, with the new additions being: SocGholish, NanoCore, ZPHP, Jinupd, and Pegasus.

> From July 2023 through December 2024, SocGholish was the top malware affecting K-12 entities, making up 60% of the top 10 malware.

SocGholish is a downloader written in JavaScript which is distributed through malicious or compromised websites. SocGholish uses fake software updates, specifically browser updates, to trick users into downloading the malware. The malware uses multiple methods for traffic redirection and payload delivery. After initial infection, the cyber threat actors (CTAs) use Cobalt Strike, leverage PowerShell, and steal information from the victim's system. Additionally, SocGholish infections can lead to further exploitation, such as installing the NetSupport remote access tool, AsyncRAT, and ransomware in some cases.

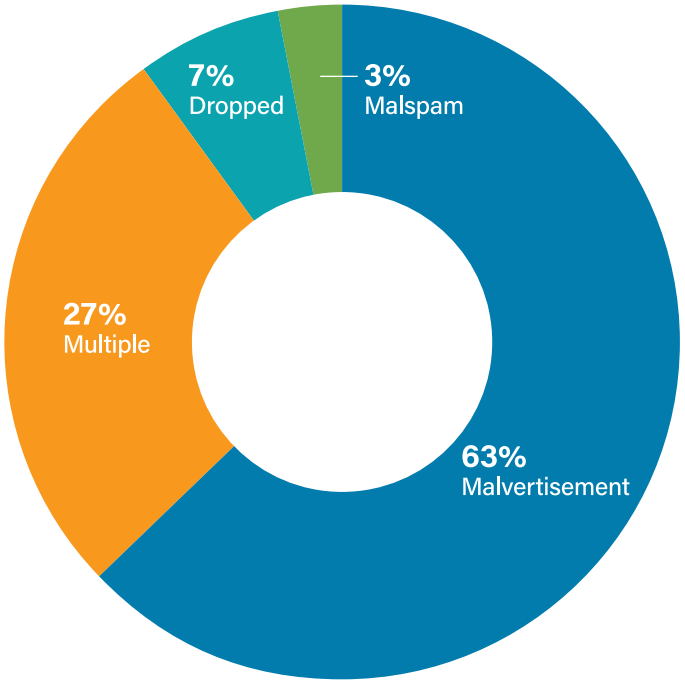


NanoCore is a Remote Access Trojan (RAT) sold on the dark web and is typically spread via malspam with an attachment. NanoCore has keylogging and screen capture capabilities, steals passwords, can download and execute files, exfiltrate data, and adds registry keys for persistence.

CoinMiner is a cryptocurrency miner family that typically uses Windows Management Instrumentation (WMI) to spread across a network. Additionally, it often uses the WMI Standard Event Consumer scripting to execute scripts for persistence. However, the malware's capabilities vary as there are multiple variants. CoinMiner spreads through malspam or is dropped by other 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.



Malvertisement made up 63% of the top malware initial infection vectors prodominately due to the ongoing SocGholish campaign. Multiple, which was the top initial infection vector in last year's report, continues to increase and make up a significant percentage due to CTAs utilizing more than one vector to increase their chances of success. The most popular combination for the multiple initial infection vector is malspam and dropped. Dropped and malspam continue to close out the rest of the top 10 malware initial infection vectors.

63%

Malvertisement

Malware introduced through malicious advertisements. Malware currently using this technique include SocGholish and ZPHP.

27%

Multiple

Malware that currently uses at least two vectors, such as dropped and malspam. Malware currently using this technique include Amadey, ArechClient2, CoinMiner, and Lumma Stealer.

7%

Dropped

Malware delivered by other malware already on the system, an exploit kit, infected third-party software, or manually by a CTA. Malware currently using this technique include Gh0st and Ratenjay.

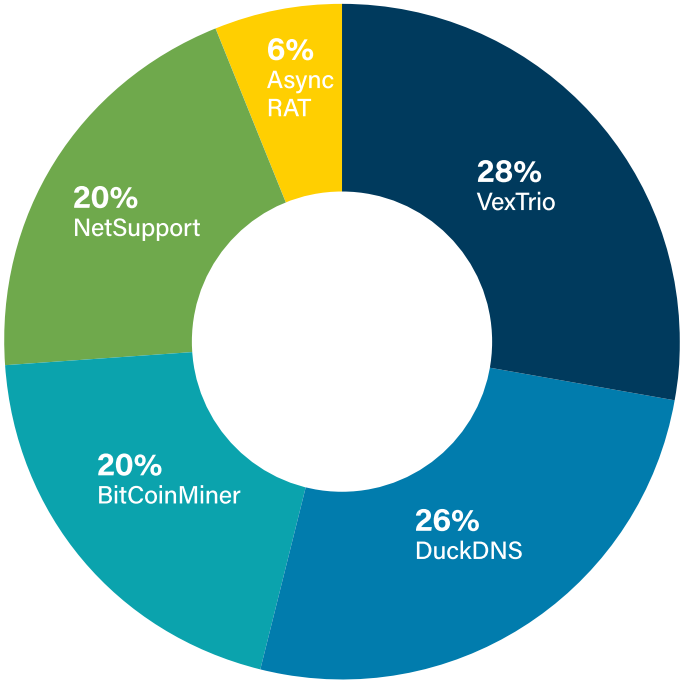
3%

Malspam

Unsolicited emails, which either direct users to malicious websites or trick users into downloading or opening malware. Malware currently using this technique include Agent Tesla and Tinba.

Top 5 Non-Malware

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. Four of the top 5 non-malware threats are legitimate tools or services, making up 72% of the top 5 non-malware threats. These legitimate tools or services include: AsyncRAT, BitCoinMiner, DuckDNS, and NetSupport.



From July 2023 through December 2024, three of the top 5 non-malware changed from the previous year's MS-ISAC K-12 Cybersecurity Report, with the exception of AsyncRAT and NetSupport. The top two non-malware threats affecting K-12 entities were VexTrio and BitCoinMiner, making up 54% of the top 5 non-malware. VexTrio led the top 5 non-malware due to being used by multiple malware campaigns, such as SocGholish. BitCoinMiner moved to the second spot which is likely due to the surge in the price of bitcoin over the past year.

VexTrio is the name of a CTA traffic broker group as well as the group's infrastructure. They operate traffic distribution systems (TDSs), as well as their own infrastrucutre. VexTrio also sells the use of their TDSs to affiliate CTAs, which is known as TDS-as-a-Service. Affiliate CTAs will direct traffic from compromised websites to the VexTrio TDS infrastructure, which is then redirected to various malicious websites based on the traffic profile attributes.

DuckDNS is a legitimate DDNS or dynamic DNS serivce. DuckDNS is a free service which will point a DNS (subdomain of duckdns[.]org) to an IP address of your choice. However, CTAs often use DuckDNS service, as well as other services like DuckDNS, to deliver malware and for comand and control infrastructure.

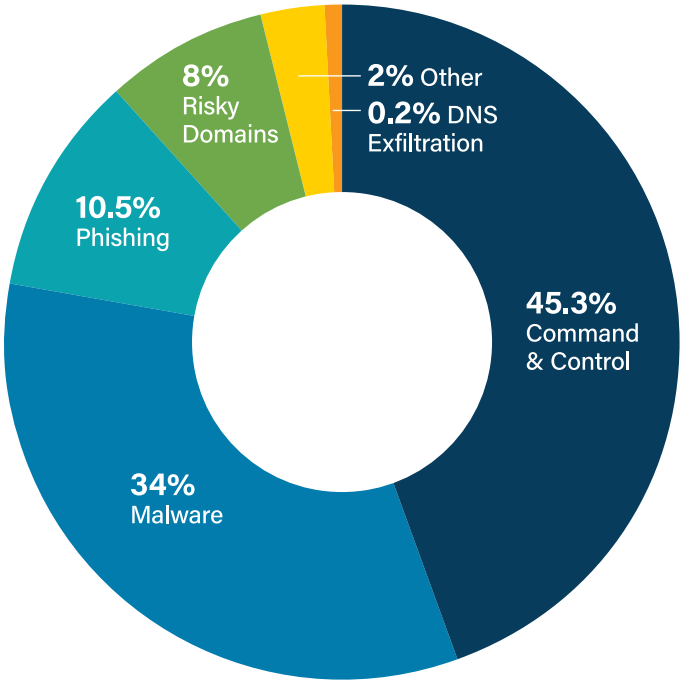
BitCoinMiner is a legitimate cryptocurrency miner that CTAs are deploying on unauthorized computers and networks. BitCoin Miners utilize the processing power of the host machine to mine BitCoin, which degrades the performance on the host for legitimate applications.

Four of the top 5 non-malware threats are legitimate tools or services, making up 72% of the top 5 non-malware threats. These legitimate tools or services include: AsyncRAT, BitCoinMiner, DuckDNS, and NetSupport.

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 July 2023 through December 2024, command and control ("C&C") overtook "malware" as the top-ranking spot for MDBR blocked activity. C&C activity increased year over year by 1,552%, while Malware blocked activity increased by 443%. Although Malware activity did increase over the past year, it did not increase enough to keep the top spot.



Between July 2023 through December 2024, command and control ("C&C") overtook "malware" as the top ranking spot for MDBR blocked activity.

Appendix G: Contributors

Center for Internet Security thanks the following contributors, without whom this report would not have come to fruition:

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.

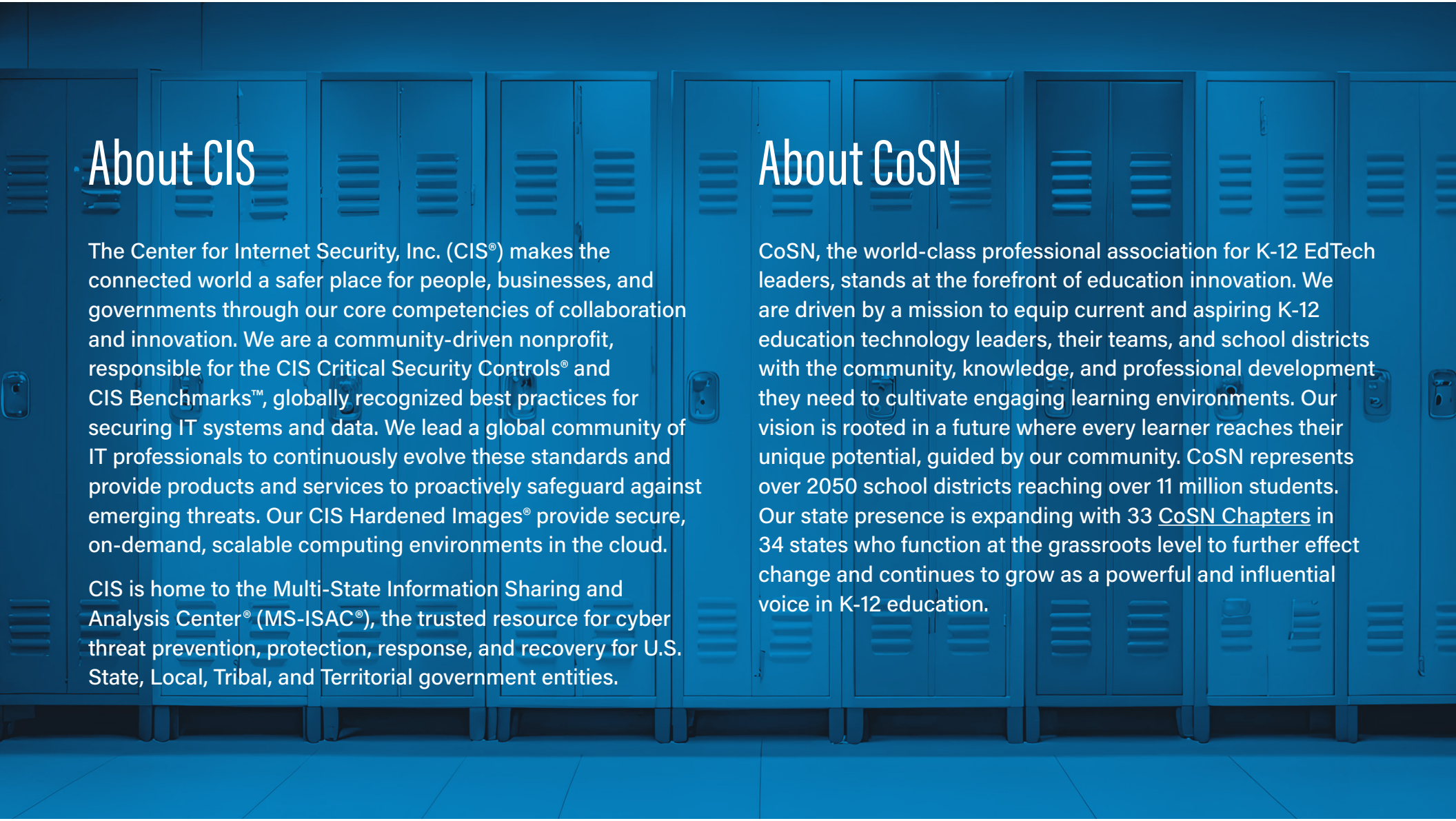
CIS Marketing and Communications Team: The Marketing and Communications Team played a pivotal role in crafting and conveying the message of this report, ensuring its clarity and reach.

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 overstated. 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.

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.



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.

About CoSN

CoSN, the world-class professional association for K-12 EdTech leaders, stands at the forefront of education innovation. We are driven by a mission to equip current and aspiring K-12 education technology leaders, their teams, and school districts with the community, knowledge, and professional development they need to cultivate engaging learning environments. Our vision is rooted in a future where every learner reaches their unique potential, guided by our community. CoSN represents over 2050 school districts reaching over 11 million students. Our state presence is expanding with 33 CoSN Chapters in 34 states who function at the grassroots level to further effect change and continues to grow as a powerful and influential voice in K-12 education.

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

CoSN

Leading Education Innovation

2025 STATE CYBERSECURITY LEGISLATION REPORT

CoSN.org

Contents

CoSN's Mission:

CoSN provides current and aspiring K-12 education technology leaders with the community, knowledge, and professional development they need to create and grow engaging learning environments.

www.cosn.org

For access to this report, please visit
www.cosn.org/cybersecurity

CoSN's work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License.

I'm pleased to share with you the **2025 State Cybersecurity Legislation Report**, CoSN's latest policy report exploring how state lawmakers are stepping up to protect schools in the face of growing cyber threats.

In 2025, school districts continue to face increasingly complex and costly cybersecurity challenges—yet most remain under-resourced and underprepared. As this report shows, while federal support is shrinking, several states are advancing innovative, bipartisan legislation to help safeguard student data, improve incident response, expand insurance access, and build the cybersecurity workforce we urgently need.

This analysis highlights the legislative activity in Arkansas, Massachusetts, Oregon, Pennsylvania, and Texas—not just to inform, but to inspire. These states represent a range of governance models and policy contexts, yet their common strategies offer actionable ideas for state and district leaders across the country. Our goal is to equip the education community with insights that move us from reactive to resilient.

I encourage you to use this report as both a reference and a call to action. Whether you're advocating for resources, updating local policies, or building new partnerships, this report underscores the importance of system-wide collaboration and strategic leadership.

Thank you for your ongoing commitment to securing the future of digital learning.

I also hope you will explore the many public resources that CoSN, the professional association of school system technology leaders/CIO/CTOs, makes available on cybersecurity at www.cosn.org/cybersecurity.

Sincerely,

Keith Krueger
CEO, CoSN

Introduction

Cybersecurity threats to K–12 schools are growing in frequency, sophistication, and cost according to the Cybersecurity and Infrastructure Security Agency and other government and private sector sources. Yet, many school districts remain under-resourced and underprepared. CoSN's 2025 State of Ed Tech report notes that 61% of school districts rely on general funds, not dedicated cybersecurity budgets, to protect their networks and data (CoSN, 2025). The vast majority of current spending (78%) goes toward monitoring, detection, and response, with 44% of districts outsourcing these functions due to cost and staffing limitations. Monitoring is now the most commonly outsourced IT function in K–12, likely due to the difficulty of acquiring and maintaining in-house expertise (CoSN, 2025).

Despite these investments, most education technology leaders do not perceive their school districts to be at high risk for major cyber threats. Only 27% of districts identified phishing as a high risk, with even fewer, just 13% each, flagging unauthorized disclosure of student data or ransomware attacks as major threats (CoSN, 2025). These relatively low risk perceptions may reflect limited capacity to assess cyber threats, and do not account for the value of student data to cybercriminals, which is often more valuable than adult data due to its long-term utility on the black market (CoSN, 2025).

The K-12 cybersecurity landscape is likely to be further complicated by recent federal policy changes and funding cuts, including the Trump Administration's unilateral elimination of federal support for the Multi-State Information Sharing and Analysis Center (MS-ISAC), which had provided free cybersecurity training and coordination support to districts. Without this support, cybersecurity risks are likely to grow, especially in underfunded and understaffed districts (CoSN, 2025).

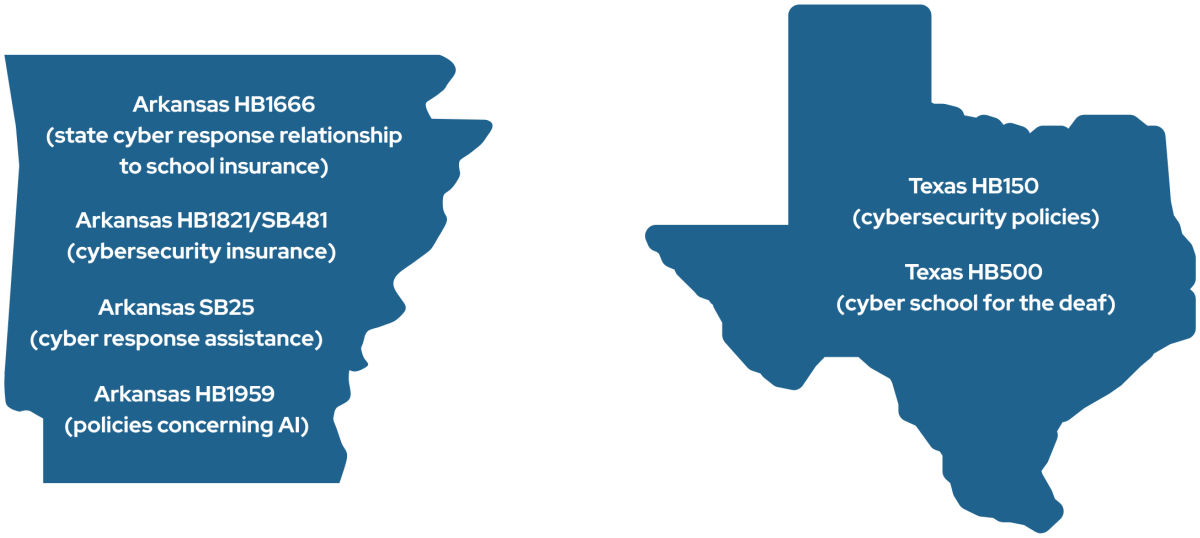
In contrast to troubling recent federal developments, some state policymakers have stepped up this year by introducing cybersecurity legislation and approving new laws that are designed to help school districts. This policy paper highlights legislative developments in five diverse states—Arkansas, Massachusetts, Oregon, Pennsylvania, and Texas—to identify common strategies and actionable insights for other state and local leaders. CoSN selected these states because they represent a range of regional, political, and governance contexts, and their recent activity reflects both mature and emerging state-level responses to K–12 and related education or public sector cybersecurity needs.

By learning from these examples, education leaders and policymakers in all states can better understand what's working, what's emerging, and how to move from fragmented, reactive approaches to systemic, resilient cybersecurity strategies.

Summary of 2025 State K-12 Focused Cybersecurity Legislation

Legislators in Arkansas (6 bills), Massachusetts (5 bills), Oregon (2 bills), and Texas (5 bills) introduced eighteen bills this year focused on improving K-12 cybersecurity. Pennsylvania did not consider any K-12 focused bills. The K-12 focused bills look beyond general government or postsecondary applicability and directly target, in some fashion, school districts, public elementary and secondary schools, education service agencies, or other K-12 institutions. Common policy themes embedded in the eighteen bills include expanding access to cybersecurity insurance, establishing enhanced training and infrastructure support, improving cyberattack responses, standardizing data practices, and requiring cyber risk assessments within K–12 systems.

Of the eighteen K-12 focused cybersecurity bills introduced in the states featured in this paper, seven were enacted but only in two states: Arkansas and Texas.



The remaining twelve bills failed to advance or were still pending as of mid-July 2025. The introduced and enacted K-12 centric bills show that lawmakers in these covered states recognize the need to strengthen schools' cyber readiness and response. A complete list of the eighteen K-12-specific bills (enacted and unenacted) follows in the next section.

K–12 Focused Cybersecurity Bills

Arkansas

Amends existing law relating to the state's cyber response program which includes school districts as participating governmental entities **(HB1666) – Enacted**

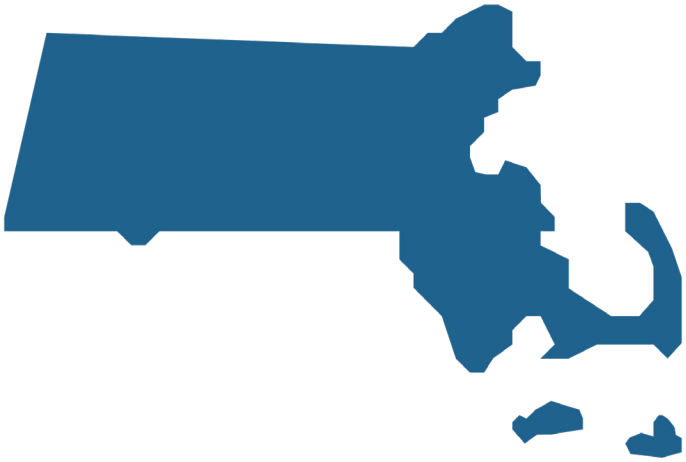
Requires the State Insurance Department to offer cybersecurity insurance for public schools and gives the Department the authority to mandate reporting requirements for districts **(HB1821) – Enacted**

Amends existing policy regarding use of technology resources and cybersecurity by public entities, including public school districts, to require creation of policies concerning the authorized use of artificial intelligence **(HB1959) – Enacted**

Expands the responsibilities of technology coordinators in education service cooperatives to include cyber incident response **(HB2002) – Not Enacted**

Appropriates funding for the Arkansas Self-Funded Cyber Response Program to assist school districts after cyberattacks **(SB25) – Enacted**

Companion to HB1821; also provides cybersecurity insurance coverage requirements for K–12 schools **(SB481) – Enacted**



Massachusetts
Prohibits employers, defined to include school districts, from using electronic monitoring tools to collect employee information - any data collected must be consistent with the state's data and cyber-privacy laws **(H77 & S35) - Pending**

Provides funds to Bellingham Public Schools for cybersecurity infrastructure as part of a larger appropriations bill **(H4227 & S2514) – Pending**

Amends school improvement planning and early education policies to include cybersecurity, privacy, and screen time limitations **(S463) – Pending**

Oregon
Directs the Department of Education to standardize student data practices and analyze cybersecurity risks in K–12 schools **(HB2508) – Pending governor's action**

Companion to HB2508; also addresses cybersecurity in student data systems for school districts and educational service districts **(SB312) – Not Enacted**

Texas
Establishes the Texas Cyber Command in place of the Department of Information Resources - amends the law to make clear that school districts must ensure cybersecurity policies do not conflict with information security standards for institutions of higher education adopted by the Texas Cyber Command; tasked with cybersecurity training, including K–12 systems **(HB150/SB2176) – Enacted**

Provides funds to the School for the Deaf for information technology and cybersecurity initiatives **(HB500) – Enacted**

Requires a state study to identify ways for school districts to improve cybersecurity and address rising costs **(SB1686) – Not Enacted**

Makes cybersecurity programs eligible under the Rural Pathway Excellence Partnership for in-person or remote instruction **(SB2132) – Not Enacted**

The Evolving State Policy Landscape

While the above bills focused more squarely on K–12 education, a broader set of legislative efforts in 2025 showed a strong state-level commitment to strengthening cybersecurity across all public sectors—including postsecondary education, state agencies, and critical infrastructure. Of the 61 total bills (K-12 focused and broader cybersecurity bills) introduced in the five studied states, most measures addressed general government systems, postsecondary institutions, or cross-cutting issues such as insurance, incident response coordination, AI accountability, and statewide workforce development. Many bills referenced multiple sectors (e.g., both K–12 and postsecondary). These broader bills illustrate a trend toward comprehensive cybersecurity governance, with several proposals creating centralized cyber commands, requiring state and local agencies to adopt baseline cyber standards, investing in higher education cybersecurity training programs, and funding response infrastructure accessible to multiple sectors—including schools.

If enacted, many of these broader policy initiatives would benefit the K–12 sector indirectly by:

- Expanding shared cybersecurity services and insurance pools;
- Establishing regional security operations centers and training pipelines involving community colleges and universities;
- Requiring coordinated incident reporting across agencies and municipalities; and
- Creating legal frameworks for data privacy and artificial intelligence accountability.

These developments suggest that states recognize cybersecurity as a systemic issue that spans education, public safety, health, and digital infrastructure. While K-12 systems remain especially vulnerable, they often now sit within a wider legislative push to modernize and secure public sector technology.

These broader legislative trends may also demonstrate a maturing state policy landscape that emphasizes proactive governance, coordinated response infrastructure, public-sector system readiness, and cybersecurity workforce development. While K–12 systems remain a clear area of concern, state leaders are often focused on policies that embed school districts within a larger framework of cyber resilience—often alongside higher education institutions, local governments, and state agencies. This activity reflects several urgent realities:

Persistent Threats: Public-sector institutions, including school districts, continue to be frequent targets of ransomware groups and other cybercriminals, with attacks growing in scale and sophistication.

Federal Encouragement and Support: Guidance and funding from the Cybersecurity and Infrastructure Security Agency (CISA), the State and Local Cybersecurity Grant Program, and emerging federal standards had been catalyzing state-level action but that trend may wane under the current administration's funding cuts.

Capacity Gaps: Many public entities, especially school districts and smaller agencies, still lack dedicated cybersecurity staff, infrastructure, and incident response protocol, prompting states to take on greater roles as policy leaders, conveners, and resource hubs.

Key Legislative Strategies in the Studied States

Several common policy strategies emerged across the cybersecurity legislation introduced or enacted in the tracked states—Arkansas, Massachusetts, Oregon, Pennsylvania, and Texas—in 2025. These strategies reflect a shared focus on improving cyber preparedness, governance, and workforce capacity in both education and broader government systems.

Common Legislative Strategies in 2025

Strategy	States
Centralized Cyber Oversight	AR, MA, PA, TX
Cyber Insurance and Risk Mitigation	AR, MA, OR, TX
Workforce Development and Education	MA, OR, TX
K–12 and Higher Ed Cyber Integration	AR, MA, TX
Incident Reporting and Crisis Response	MA, OR, PA, TX
AI and Privacy-Cyber Integration	AR, MA, TX

Centralized Cybersecurity Governance and Oversight

States are taking more steps to set up central teams to manage cybersecurity, enforce standards, and coordinate responses.

Arkansas HB1549 (Enacted): Established the State Cybersecurity Office with authority over cybersecurity functions across state agencies and designated it as a resource for local governments and educational institutions.

Texas HB150 (Enacted): Created the Texas Cyber Command to lead cybersecurity prevention, response, and coordination across governmental entities.

Pennsylvania HB1219/SB373 (Pending): Proposed the creation of an Office of Information Technology and a Joint Cybersecurity Oversight Committee.

Massachusetts S39 (Pending): Proposed a statewide Cyber Incident Response Team tasked with cross-agency planning and coordination.

Cybersecurity Insurance and Risk Management

States are working to manage cybersecurity liability and financial exposure through insurance frameworks and dedicated funds.

Arkansas HB1821/SB481 (Enacted): Requires all public school districts, education service cooperatives, and charter schools to obtain cybersecurity insurance and gives the State Insurance Department the authority to require each entity to submit program reports.

Oregon HB3228 (Not Enacted): Proposed a Cybersecurity Resilience Fund to support public bodies—especially those unable to meet cyber insurance requirements—via the Cybersecurity Center of Excellence.

Massachusetts H3363 (Pending): Encouraged preference for IT vendors with cybersecurity insurance during state procurement.

Cybersecurity Workforce Development and Education

Many states are investing in career pathways and training infrastructure to address the cybersecurity talent gap.

Massachusetts H3983/H4227 (Pending): Proposed funding for cybersecurity workforce programs, including cyber ranges and scholarships, with a focus on equity and partnerships with community colleges.

Oregon HB3228 (Not Enacted): Directed funding to improve IT systems and enhance cybersecurity readiness across state agencies, with implementation support through the Higher Education Coordinating Commission.

Integration of Cybersecurity into K–12 and Higher Education Policy

States are embedding cybersecurity readiness and risk mitigation policies into the education sector—especially at the district and institutional level.

Arkansas HB1821 (Enacted): Would mandate cybersecurity risk insurance coverage and allows for reporting for public school systems.

Massachusetts S463 (Pending): Would incorporate cybersecurity, privacy, and screen time benchmarks into school improvement plans and require early childhood educator training on digital safety.

Texas SB1686 (Not Enacted): Would require a state study to assess school districts' cybersecurity needs and rising costs.

Incident Reporting and Crisis Response Readiness

There is growing emphasis on incident preparedness, real-time reporting, and ensuring public entities have playbooks for rapid response.

Massachusetts HD4360 (Pending): Would require all municipalities and school districts to report cybersecurity incidents to the state's operations center.

Texas HB3112 (Enacted): Would allow government bodies to discuss cybersecurity policies related to critical infrastructure in closed meetings, enhancing confidentiality during crisis response.

Pennsylvania HB1219 (Pending): Would add situational awareness and threat coordination as core duties of the proposed Office of Information Technology.

AI, Privacy, and Cybersecurity Intersections

States are proactively aligning cybersecurity strategies with emerging technologies like artificial intelligence and digital privacy regulation.

Massachusetts S2516/H104 (Pending): Proposes a comprehensive data privacy framework requiring cybersecurity safeguards and risk-based limits on personal data collection.

Arkansas HB1959 (Enacted): Requires all public entities, including school districts, to adopt policies governing the authorized use of artificial intelligence.

Texas HB1709 (Not Enacted): Would require cybersecurity impact assessments for high-risk AI systems deployed by state agencies.

Policy Recommendations for State and Local Education Leaders

Looking at the cybersecurity measures introduced this year in the five studied states, we recommend that state and local leaders consider adopting policies and practices across a number of areas including improving governance, funding risk assessments, expanding the cybersecurity workforce, requiring reporting and response readiness, and modernizing procurement and data standards. In each of these areas, policymakers should consider K-12 schools' cybersecurity needs and aim to address them.

Establish or Strengthen Statewide K–12 Cybersecurity Governance

Recommendation: Designate a cybersecurity lead within the state education agency and ensure that school districts are included in state-level cybersecurity planning and governance bodies.

State Examples:

Arkansas enacted multiple bills in 2025 including one that centralized cybersecurity oversight in a newly empowered State Cybersecurity Office **(HB1549).** This office is responsible for setting statewide policies, including those that impact school districts.

Texas created the Texas Cyber Command **(HB150)**, a centralized structure charged with coordinating prevention, detection, and response for cybersecurity incidents across government—including education systems.

Pennsylvania introduced legislation to establish an Office of Information Technology and a Joint Cybersecurity Oversight Committee **(HB1219, SB373)**, which would guide statewide cybersecurity governance and coordinate policy across agencies, including education.

Fund and Require School District Cybersecurity Risk Assessments

Recommendation: Allocate funding for school districts to conduct risk assessments and develop mitigation strategies. Consider state-run insurance pools or financial support mechanisms.

State Examples:

Arkansas enacted legislation **(HB1821/SB481)** requiring school districts to report on their cybersecurity insurance status and authorized the State Insurance Department to manage a program covering district cybersecurity risks.

Oregon proposed the Cybersecurity Resilience Fund **(HB3228)**, which would help public bodies, including school districts, afford insurance and address security gaps.

Texas included cybersecurity risk and insurance reviews in bills requiring evaluations of agency IT systems **(HB1500, SB2404)**, laying groundwork for broader assessment programs.

Align Workforce Policy with K–12 Needs

Recommendation: Support teacher certification in cybersecurity and create K–12 student pathways aligned with current and emerging workforce demand.

State Examples:

Massachusetts introduced legislation to invest in cybersecurity workforce development, including funding for cyber ranges, scholarships, paid internships, and public awareness campaigns **(H3983, S49).**

Texas passed or introduced several bills **(HB1527, SB2097, SB2132)** including measures to expand tuition exemptions and career pathway programs to include students and educators in cybersecurity-related fields.

Oregon legislation **(HB3228)** would fund training through the Cybersecurity Center of Excellence, targeting both public agencies and education partners.

Mandate Incident Reporting and Create Response Protocols

Recommendation: Require timely reporting of cybersecurity incidents and support districts with coordinated response plans and training exercises.

State Examples:

Massachusetts introduced legislation **(HD4360)** requiring cities, towns, and school districts to report known cybersecurity incidents to the Commonwealth's Security Operations Center.

Texas passed **HB3112**, permitting governmental bodies—including school boards—to deliberate on cybersecurity matters in closed session, helping them develop response plans without exposing sensitive information.

Arkansas updated its Freedom of Information Act **(SB227)** to allow executive sessions for discussing cybersecurity breaches.

Update Procurement and Data Governance Standards

Recommendation: Require that vendors meet minimum cybersecurity standards and align procurement processes with national frameworks (e.g., NIST, CIS).

State Examples:

Massachusetts considered legislation **(H3363)** requiring state agencies, including those procuring education technology, to give preference to vendors that carry cybersecurity insurance—helping enforce a security baseline through procurement.

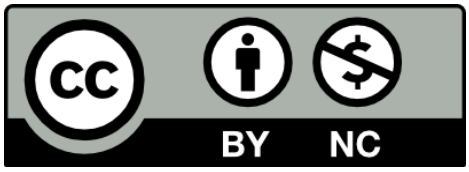
Texas passed **HB5331**, ensuring that no contract language in cybersecurity or IT service contracts can restrict a public entity's compliance with state cybersecurity law—effectively preventing vendors from blocking governance or enforcement.

Oregon considered legislation **(HB2508, SB312)** would require education agencies to standardize data governance practices, with attention to cybersecurity risks in the handling of student data.

Conclusion

State and local education leaders face mounting pressure to secure digital learning environments against increasingly sophisticated cyber threats. The 2025 legislative actions reviewed in this paper provide ideas for developing and adopting policies that will help school districts and their partners address this challenge. By adopting well designed strategies – centralized oversight, insurance requirements, workforce investment, integrated planning, and responsible innovation oversight– states can help their school districts move from reactive to resilient. Cross-sector collaboration and sustained investment will be critical to protecting students, educators, and the integrity of public education systems. For further information, please visit CoSN's website to review our Cybersecurity Project's many related cybersecurity resources.

Permission is granted under a Creative Commons Attribution + Non-commercial License to replicate, copy, distribute, and transmit this report for non-commercial purposes with attribution given to CoSN.



CoSN
Leading Education Innovation

Federal Bureau of Investigation
Internet Crime Report
2024

INTERNET CRIME COMPLAINT CENTER

CONTENTS

Dear Reader:

This year marks the 25th anniversary of the FBI's Internet Crime Complaint Center, or IC3. Originally intended to serve the law enforcement community, IC3 has evolved to become the primary destination for the public to report cyber-enabled crime and fraud as well as a key source for information on scams and cyber threats. Since its founding, IC3 has received over 9 million complaints of malicious activity. During its infancy, IC3 received roughly 2,000 complaints every month. For the past five years, IC3 has averaged more than 2,000 complaints every day.

As nearly all aspects of our lives have become digitally connected, the attack surface for cyber actors has grown exponentially. Scammers are increasingly using the Internet to steal Americans' hard-earned savings. And with today's technology, it can take mere taps on a keyboard to hijack networks, cripple water systems, or even rob virtual exchanges. Cryptocurrency has become an enticing means to cheat investors, launder proceeds, and engage in other illicit schemes.

Last year saw a new record for losses reported to IC3, totaling a staggering $16.6 billion. Fraud represented the bulk of reported losses in 2024, and ransomware was again the most pervasive threat to critical infrastructure, with complaints rising 9% from 2023. As a group, those over the age of 60 suffered the most losses and submitted the most complaints.

These rising losses are even more concerning because last year, the FBI took significant actions to make it harder, and more costly, for malicious actors to succeed. We dealt a serious blow to LockBit, one of the world's most active ransomware groups. Since 2022, we have offered up thousands of decryption keys to victims of ransomware, avoiding over $800 million in payments.

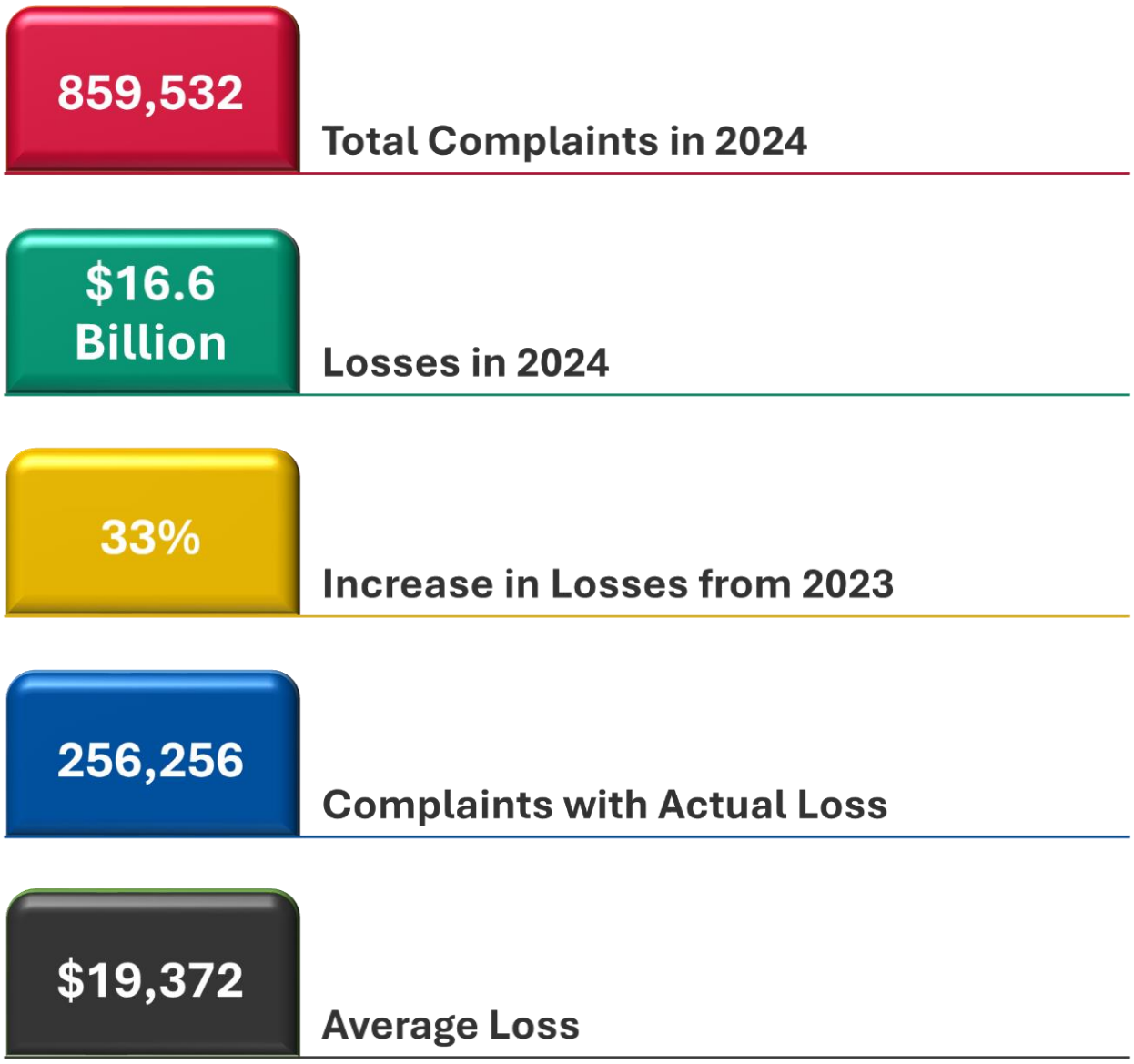
Also in 2024, we worked proactively to prevent losses and minimize victim harm through private sector collaboration and initiatives like Operation Level Up. We disbanded fraud and laundering syndicates, shut down scam call centers, shuttered illicit marketplaces, dissolved nefarious "botnets," and put hundreds of other actors behind bars. Our partnerships across the intelligence, law enforcement, and private sector communities have never been stronger.

The criminals Americans face today may look different than in years past, but they still want the same thing: to harm Americans for their own benefit. This brings me back to IC3's quarter-century milestone. While the top threats facing our country have certainly shifted over the decades, protecting American citizens—whether that means your safety, your money, or your data—remains a cornerstone of the FBI's mission.

And in the fight against increasingly savvy criminals, the FBI also relies on *you*. Without the information you report to us through IC3 or your local FBI Field Office, we simply cannot piece together the puzzle of this ever-shifting threat landscape. If ever you suspect you're a victim of cyber-enabled crime, do not hesitate to let us know. We want to be there for you, and what you report will help us help others.

B. Chad Yarbrough
Operations Director for Criminal and Cyber
Federal Bureau of Investigation

2024 BY THE NUMBERS[1]

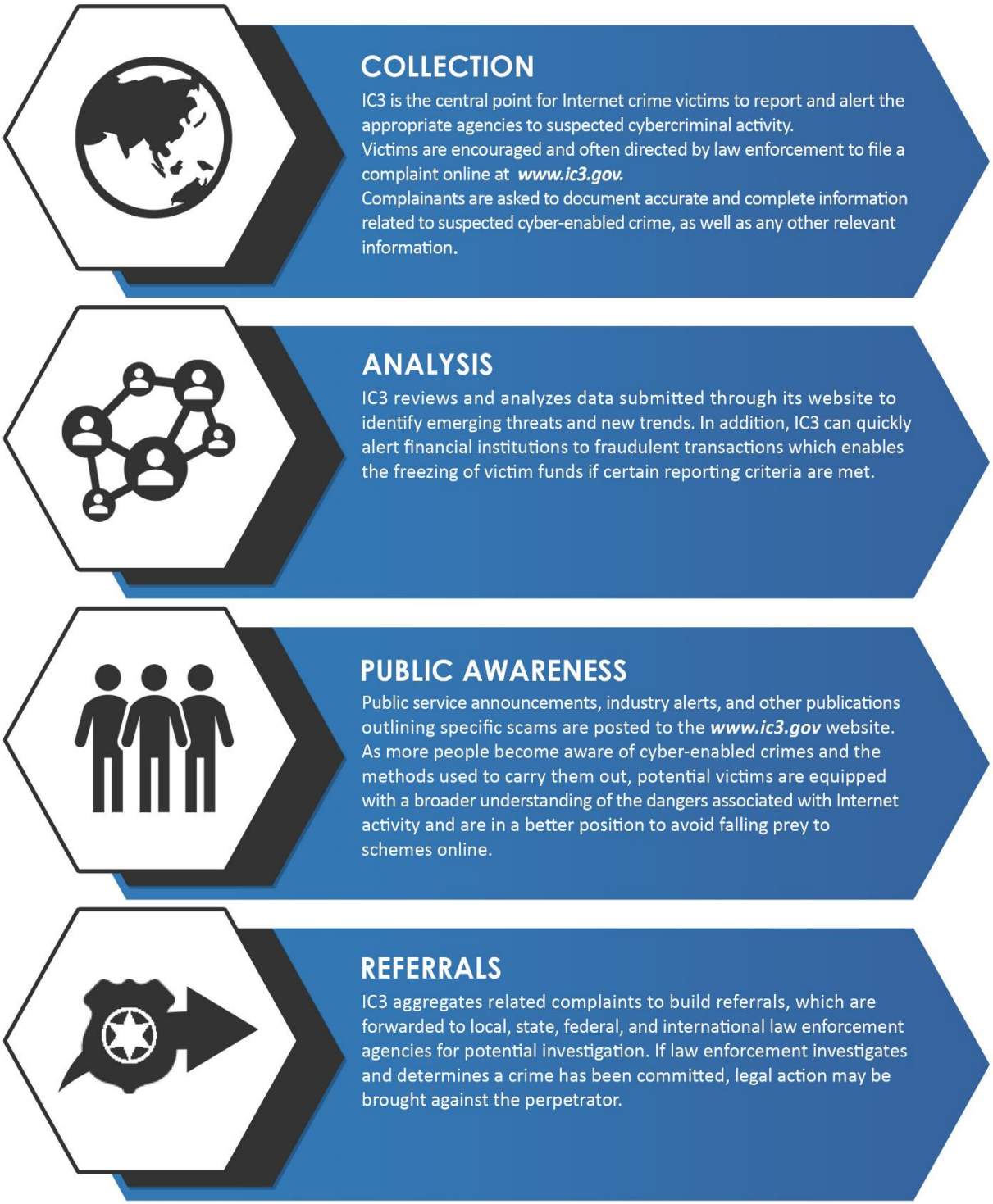


[1] Accessibility description: Image depicts key statistics regarding complaints and losses. In 2024, complaints totaled 859,532, with losses of $16.6 billion, representing a 33 percent increase from 2023. 256,256 complaints reported an actual loss. For complaints, the average reported loss was $19,372.

IC3's ROLE IN COMBATTING CYBER CRIME[2]

[2] Accessibility description: Image lists 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 FBI's LEEP website.

IC3 CORE FUNCTIONS[3]



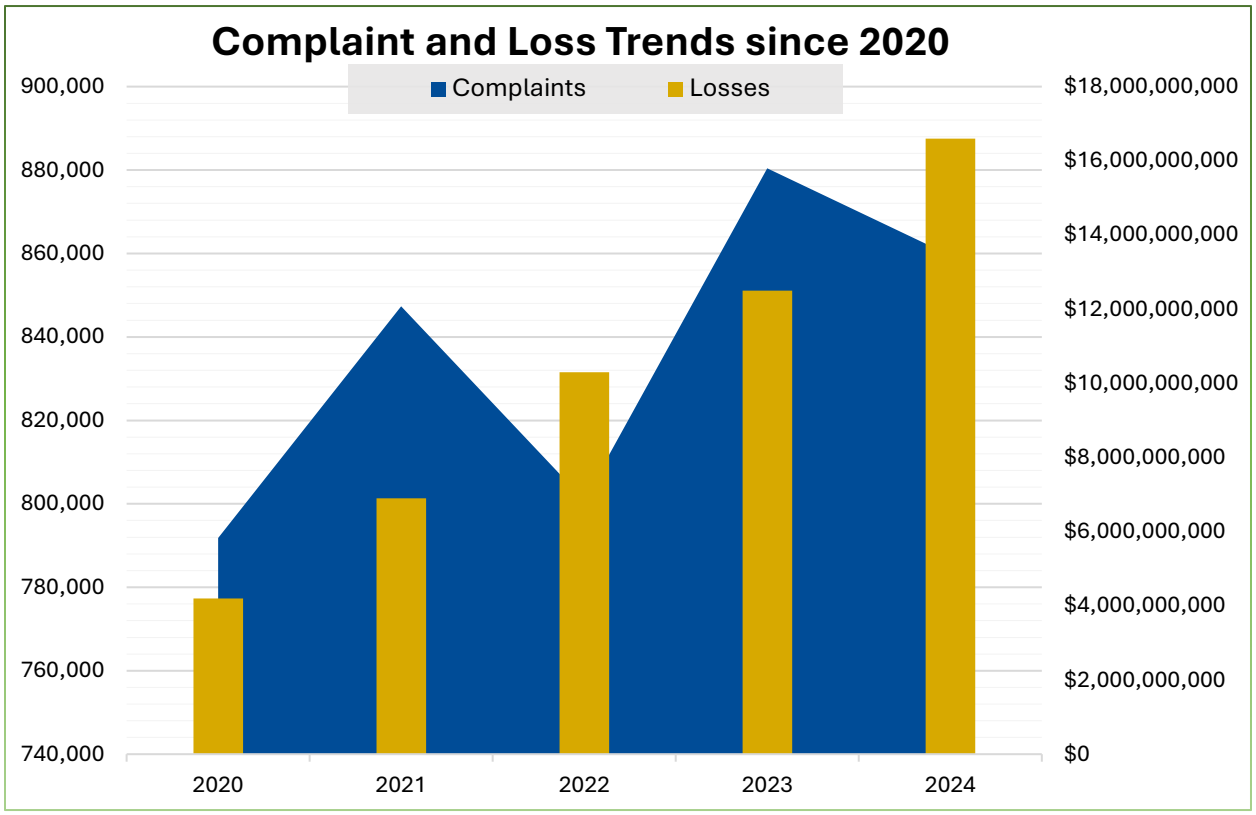
[3] Accessibility description: Image contains icons with the core functions. Core functions - Collection, Analysis, Public Awareness, and Referrals - are listed in individual blocks as components of an ongoing process.

IC3 COMPLAINT STATISTICS

PAST FIVE YEARS

IC3 has received an average of 836,000 complaints per year. These complaints address a wide array of Internet scams affecting individuals around the globe.

[4]



[5]

IC3 COMPLAINTS - PAST FIVE YEARS

4.2 Million Complaints

$50.5 Billion in Losses

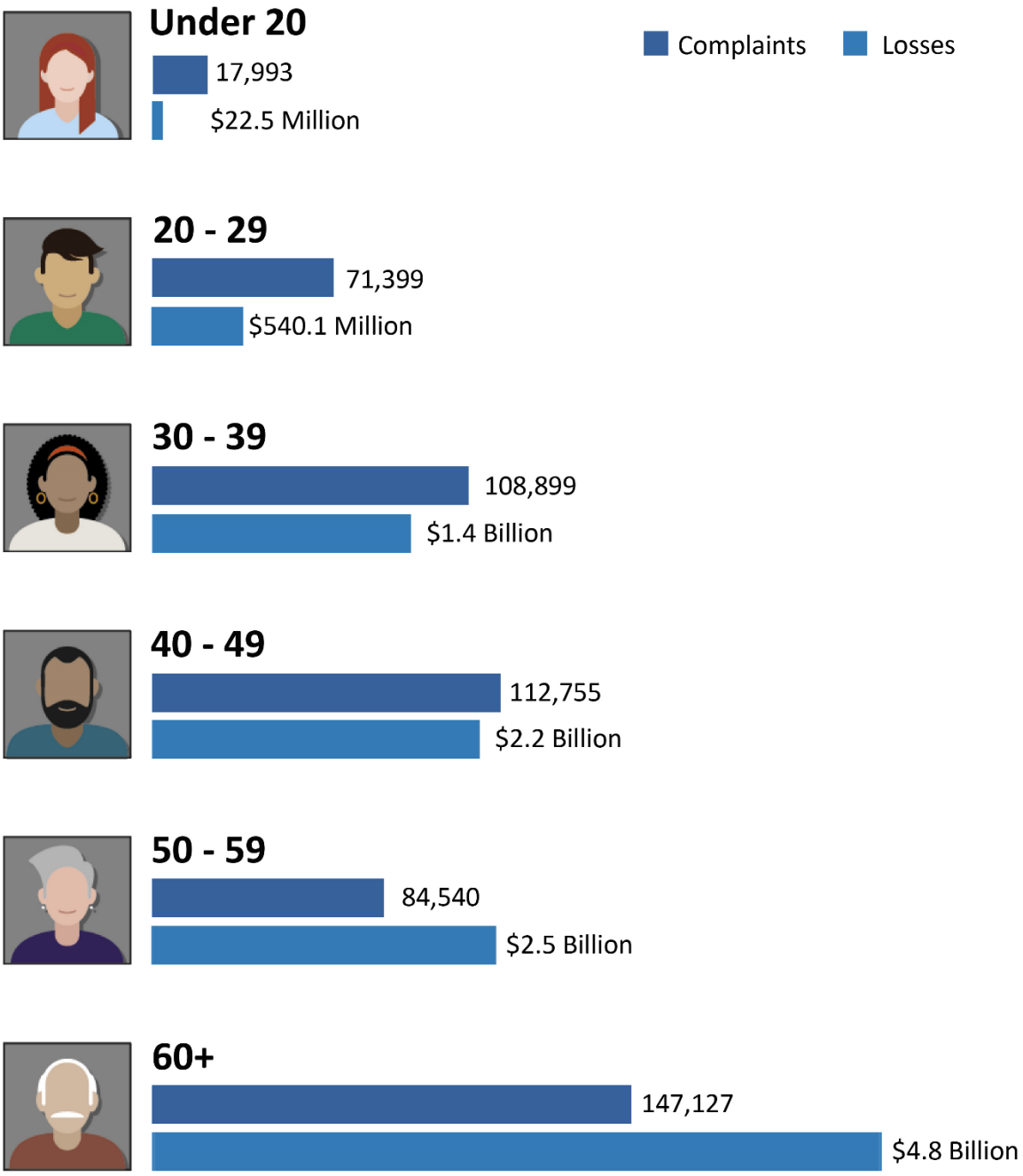
836,000 Average

Since 2000, the IC3 has received more than 9 million complaints.

[4] Accessibility description: Chart describes complaint counts and losses over a 5-year period.

[5] Accessibility description: Chart includes yearly and aggregate data for complaints and losses over the years 2020 to 2024. Over this time, IC3 received a total of 4.2 million complaints, a reported loss of $50.5 billion, and an average of 836,000 complaints received per year. Since 2000, IC3 has received more than 9 million complaints. * Please see Appendix C for more information regarding IC3 data.

2024 COMPLAINTS BY AGE GROUP [6]



[6] Not all complaints include an associated age range—those without this information are excluded from this table. Please see Appendix C for more information regarding IC3 data. Accessibility description: Chart shows number of complaints and losses by age group. Under 20: 17,993 complaints, $22.5 million in losses; 20-29: 71,399 complaints, $540.1 million in losses; 30-39: 108,899 complaints, $1.4 billion in losses; 40-49: 112,755 complaints, $2.2 billion in losses; 50-59: 84,540 complaints, $2.5 billion in losses; 60+: 147,127 complaints, $4.8 billion in losses.

2024 CRIME TYPES

BY COMPLAINT COUNT

Crime Type	Complaints	Crime Type	Complaints
Phishing/Spoofing	193,407	**Harassment/Stalking**	11,672
Extortion	86,415	**Real Estate**	9,359
Personal Data Breach	64,882	**Advanced Fee**	7,097
Non-Payment/ Non-Delivery	49,572	**Crimes Against Children**	4,472
Investment	47,919	**Lottery/Sweepstakes/ Inheritance**	3,690
Tech Support	36,002	**Data Breach**	3,204
Business Email Compromise	21,442	**Ransomware**	3,156
Identity Theft	21,403	**Overpayment**	2,705
Employment	20,044	**IPR*/Copyright and Counterfeit**	1,583
Confidence/Romance	17,910	**Threats of Violence**	1,360
Government Impersonation	17,367	**SIM Swap**	982
Credit Card/Check Fraud	12,876	**Botnet**	587
Other	12,318	**Malware**	441
*Descriptor***			
Cryptocurrency	149,686		

*IPR: Intellectual Property Rights

** This descriptor relates to the medium or tool used to facilitate the crime and used by IC3 for tracking purposes only. It is available as a descriptor only after a crime type has been selected.

Please see Appendix C for more information regarding IC3 data.

2024 CRIME TYPES *continued*

BY COMPLAINT LOSS

Crime Type	Loss	Crime Type	Loss
Investment	$6,570,639,864	**Extortion**	$143,185,736
Business Email Compromise	$2,770,151,146	**Lottery/Sweepstakes/ Inheritance**	$102,212,250
Tech Support	$1,464,755,976	**Advanced Fee**	$102,074,512
Personal Data Breach	$1,453,296,303	**Phishing/Spoofing**	$70,013,036
Non-Payment/Non-Delivery	$785,436,888	**SIM Swap**	$25,983,946
Confidence/Romance	$672,009,052	**Overpayment**	$21,452,521
Government Impersonation	$405,624,084	**Ransomware ***	$12,473,156
Data Breach	$364,855,818	**Harassment/Stalking**	$10,611,223
Other	$280,278,325	**Botnet**	$8,860,202
Employment	$264,223,271	**IPR/Copyright and Counterfeit**	$8,715,512
Credit Card/Check Fraud	$199,889,841	**Threats of Violence**	$1,842,186
Identity Theft	$174,354,745	**Malware**	$1,365,945
Real Estate	$173,586,820	**Crimes Against Children**	$519,424

*Descriptor***	
Cryptocurrency	$9,322,335,911

* 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 FBI, thereby creating an artificially low overall ransomware loss rate. Lastly, the number only represents what entities report to FBI via IC3 and does not account for the entity directly reporting to FBI field offices/agents.

** This descriptor relates to the medium or tool used to facilitate the crime and is used by IC3 for tracking purposes only. It is available as a descriptor only after a crime type has been selected.

Please see Appendix C for more information regarding IC3 data.

CYBER-ENABLED FRAUD

Cyber-enabled fraud includes complaints where criminals use the Internet or other technology to commit fraudulent activities, often involving the theft of money, data, or identity, or the creation of counterfeit goods or services. Cyber-enabled fraud is responsible for almost 83% of all losses reported to IC3 in 2024. [7]

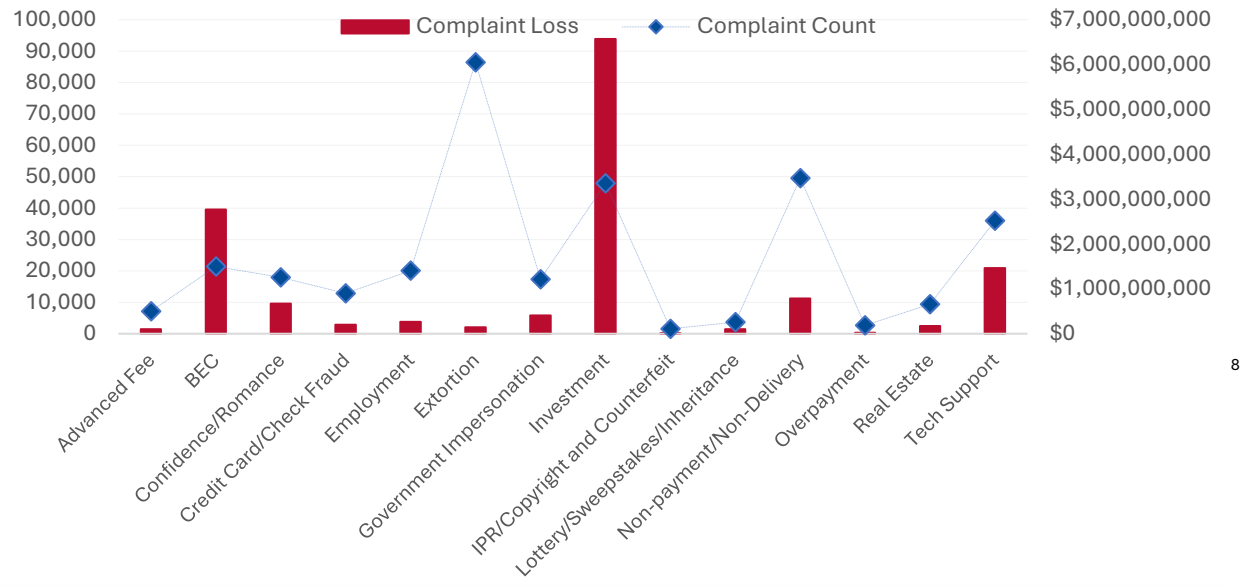
CYBER-ENABLED FRAUD in 2024

333,981 Complaints

$13.7 Billion Losses

38% of 2024 Complaints

83% of 2024 Losses



[8]

TRENDS

Call Center Scams

53,369 complaints; $1.9 billion in losses

FBI Warns of Scammers Impersonating Cryptocurrency Exchanges

Increase in Tech Support Scams Targeting Older Adults and Directing Victims to Send Cash...

Emergency Scams

357 complaints; $2.7 million in losses

FBI Warns of Scammers Targeting Senior Citizens in Grandparent Scams...

Telephone Scam Alleging a Relative is in a Financial or Legal Crisis

Toll Scams

59,271 complaints; $129,624 in losses

Smishing Scam Regarding Debt for Road Toll Services

Gold Courier Scams

525 complaints; $219 million in losses

Scammers Use Couriers to Retrieve Cash and Precious Metals...

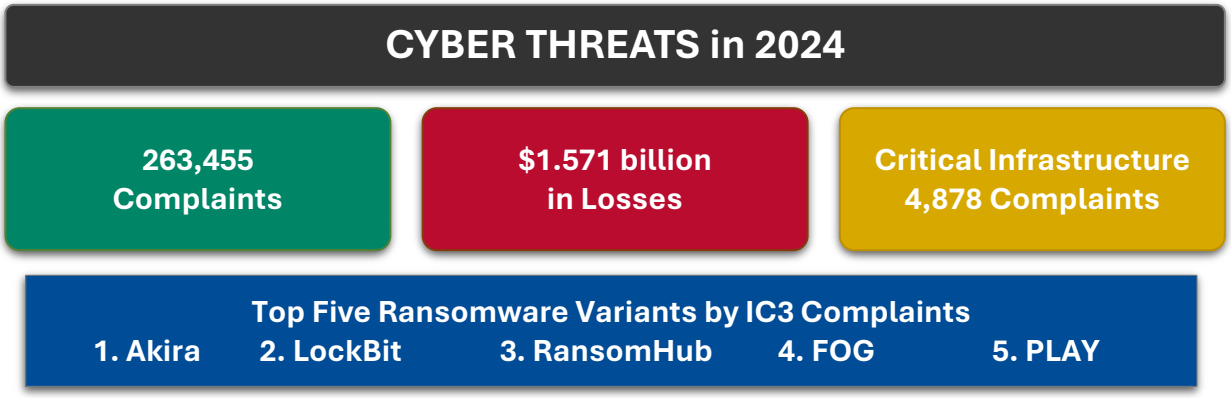
[7] Accessibility description: Chart describes totals for crime types generally considered to be cyber-enabled fraud: 333,981 complaints; $13.7 billion in losses; 38% of 2024 complaints received; 83% of 2024 losses. * Please see Appendix C for more information regarding IC3 data.

[8] Accessibility description: Chart describes counts and losses for crime types generally considered to be cyber-enabled fraud.

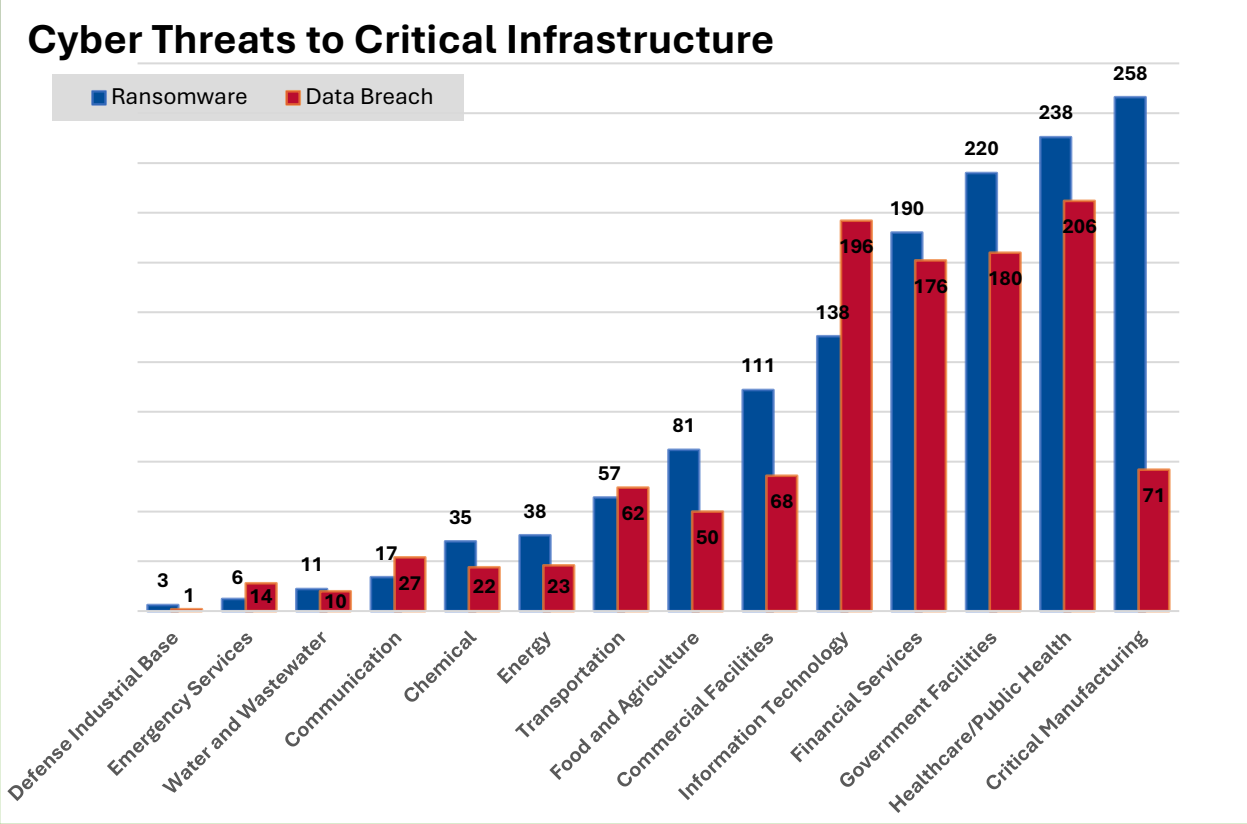
CYBER THREATS

A cyber or cybersecurity threat is a malicious act that seeks to damage data, steal data, or disrupt digital life in general. Cyber threats include ransomware, viruses and malware, data breaches, Denial of Service (DoS) attacks, and other attack vectors. IC3 received more than 4,800 complaints from organizations belonging to a critical infrastructure sector that were affected by a cyber threat. The most reported cyber threats among critical infrastructure organizations were ransomware and data breaches.

[9]



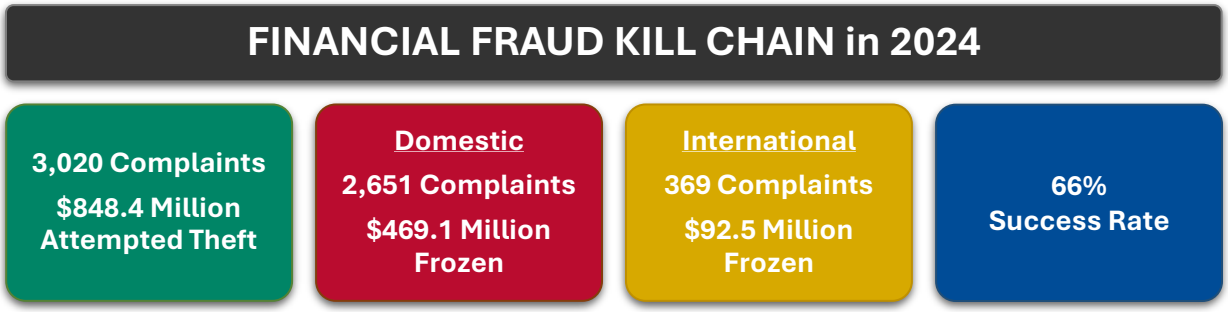
[10]



[9] Accessibility description: This chart outlines cyber threat complaints in 2024: 263,455 complaints; $1.571 billion in losses; 4,878 complaints from critical infrastructure. The five most reported ransomware variants: Akira, LockBit, RansomHub, FOG, and PLAY.

[10] Accessibility description: This chart outlines the number of ransomware and data breach complaints filed by the critical infrastructure sectors.

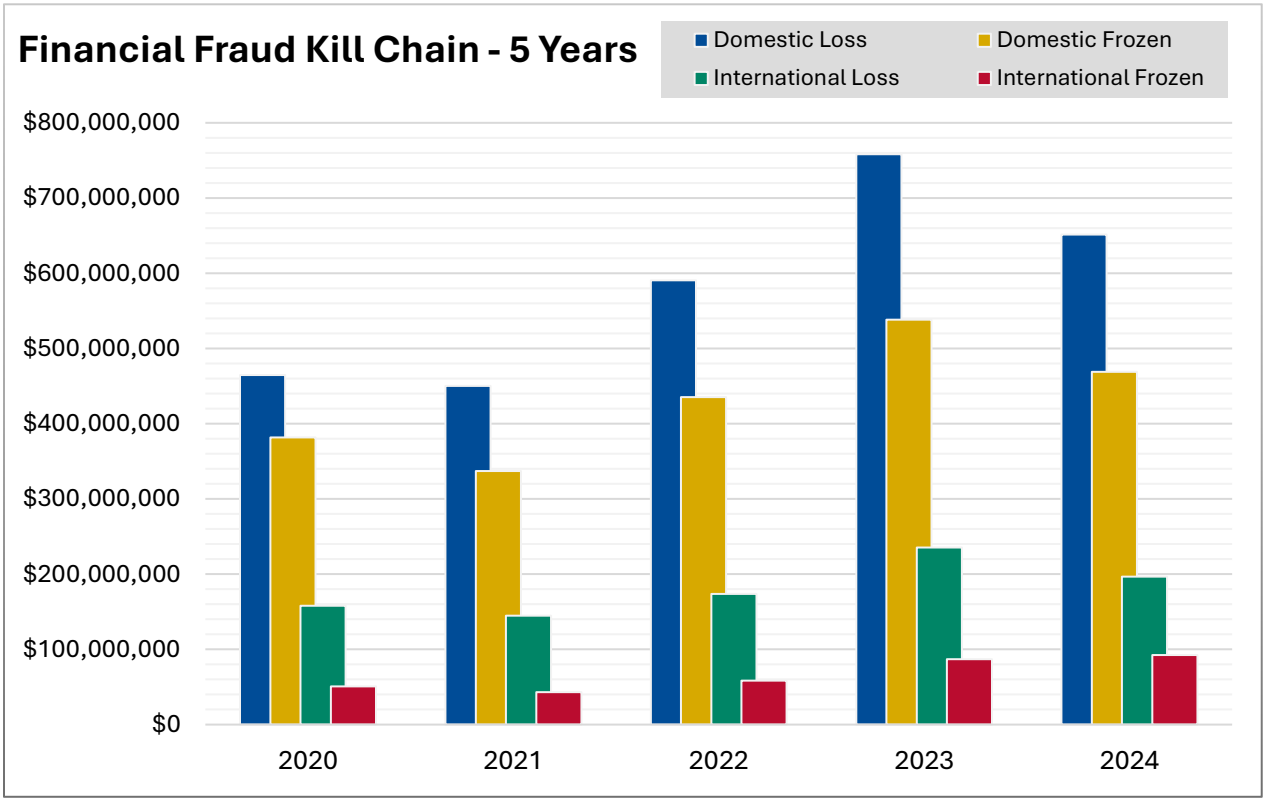
IC3 RECOVERY ASSET TEAM



[11]

Established in 2018, the IC3 Recovery Asset Team streamlines communications with financial institutions and FBI field offices to assist in the freezing of funds for victims of fraudulent domestic and international transactions via the Financial Fraud Kill Chain. Most Financial Fraud Kill Chain incidents initiated by the IC3 RAT are Business Email Compromise (BEC). The Financial Fraud Kill Chain can also be initiated for Tech Support Fraud, Romance Scams, and Data Breaches.
The Recovery Asset Team assumed responsibility for domestic-to-international transactions in April 2024. The International Financial Fraud Kill Chain is a partnership between federal law enforcement and financial entities whose purpose is to freeze fraudulent funds wired by victims. International requests are coordinated through the Financial Crimes Enforcement Network Rapid Response Team and law enforcement entities, including FBI LEGAT offices and international law enforcement partners.

[12]



[11] Accessibility description: Chart describes FFKC activity in 2024: 3,020 complaints attempted for $848.4 million. Domestic: 2,651 complaints, $469.1 million frozen; International: 369 complaints, $92.5 million frozen; 66% success rate.
[12] Accessibility description: Chart describes FFKC domestic and international frozen and loss amounts from 2020 to 2024.

POSITIVE IMPACT

Operation Level Up

Launched in January 2024, Operation Level identified victims of cryptocurrency investment fraud and notified them of the scam. The operation was initiated with the support of agents from FBI and the U.S. Secret Service. Cryptocurrency investment fraud, also known as "pig butchering," is a confidence-based scam. Subjects target victims online and develop a relationship before introducing a fraudulent investment opportunity in cryptocurrency. Victims are coached to invest more and more money into what appears to be an extremely profitable platform, only to be unable to withdraw their funds.

Success Stories

Utilizing IC3 complaint data, Operation Level Up reported:

- 4,323 victims of cryptocurrency investment fraud were notified.
- 76% of those victims were unaware they were being scammed.
- Estimated savings to victims of $285,639,989.
- 42 victims referred to an FBI victim specialist for suicide intervention.

Read More About It

Operation Level-Up: How the FBI Is Saving Victims from Cryptocurrency Investment Fraud
Operation Level Up — FBI

Call Center Fraud

Illegal call centers defraud thousands of victims each year. Two categories of call center fraud reported to the IC3 are Tech/Customer Support and Government Impersonation.

DOJ, FBI, and Central Bureau of Investigation:

Since 2022, the DOJ, FBI, and IC3 have collaborated with law enforcement in India, such as the Central Bureau of Investigation (CBI) in New Delhi and local Indian states, to combat cyber-enabled financial crimes and transnational call center fraud.

In 2024, law enforcement in India conducted multiple call center raids, disruptions, seizures, and arrests of the individuals alleged to be involved in perpetrating these crimes.

FBI Washington Field Office participated in two media series aimed at bringing awareness to call center fraud.

Success Stories

FBI responded to over 38 requests from law enforcement in India and provided approximately 60 actionable leads.

FBI enabled over 215 arrests through 11 joint operations with the CBI and other local law enforcement in 2024. This represented a 700% increase in arrests from 2023, the first full year of the collaboration.

FBI conducted hundreds of interviews and continues to support Indian law enforcement efforts and prosecution of call centers perpetrating these frauds.

Read More About It

Tech/Customer Support and Government Impersonation

POSITIVE IMPACT

Ransomware

IC3 recognized 67 new ransomware variants in 2024. The most reported of these new variants were:

- FOG
- Lynx
- Cicada 3301
- Dragonforce
- Frag

IC3 provides this information to FBI Field Offices to help identify new ransomware variants, discover the enterprises the threat actors are targeting, and determine whether critical infrastructure is being targeted.

Success Story

FBI Boston, February 2024: Authorities seized www.warzone.ws and three related domains, which together offered for sale the Warzone RAT malware — a sophisticated remote access trojan capable of enabling cybercriminals to surreptitiously connect to victims' computers for malicious purposes. The Warzone RAT provided cybercriminals the ability to browse victim file systems, take screenshots, record keystrokes, steal victim usernames and passwords, and watch victims through web cameras, all without the victims' knowledge or permission.

Read More About It

International Cybercrime Malware Service Dismantled by Federal Authorities: Key Malware Sales and Support Actors in Malta and Nigeria Charged in Federal Indictments | United States Department of JusticeCharged in Federal Indictments

Financial Fraud Kill Chain

The IC3 Recovery Asset Team streamlines communications with financial institutions and FBI field offices to assist in the freezing of funds for victims of fraudulent domestic and international transactions.

FBI Denver, March 2024: The Recovery Asset Team received a complaint reporting a BEC involving a real estate transaction. The individuals were in the process of purchasing property and received a spoofed email from their supposed real estate agents requesting that they wire $956,342 to a U.S. domestic bank to finalize the closing. Two days after the wire was initiated, the victims realized the instructions came from a spoofed email. Upon notification, the Recovery Asset Team immediately initiated the process to freeze the fraudulent recipient bank account. The transfer of $955,060 was stopped and the money was returned to the individuals.

Success Story

LEGAT Singapore, September 2024: The Recovery Asset Team received a request from LEGAT Singapore regarding a transaction sent to a U.S. domestic recipient bank in the amount of $6,661,650 due to a BEC incident. The Recovery Asset Team initiated the Financial Fraud Kill Chain request to the domestic recipient bank, who blocked the account and froze a total of $5,100,000 for recovery. Funds not available were wired out immediately upon deposit to accounts located in Spain and China. Efforts by the domestic recipient bank were made to potentially recover those wires as well.

Read More About It

SPF | International Cooperation Leading To The Interception Of Over USD 5 Million Linked To Business Email Compromise Scam

INTERNATIONAL COMPLAINT COUNTRIES

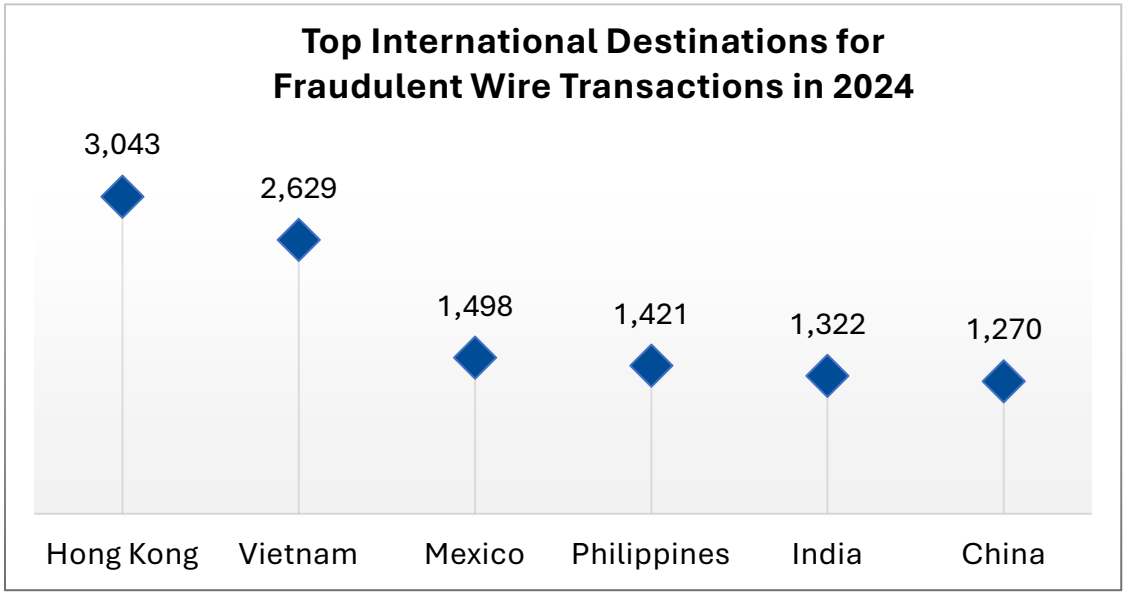
[13]

IC3 received complaints from more than 200 countries in 2024.

TOP 20 FOREIGN COUNTRIES WITH CITIZENS SUBMITTING COMPLAINTS TO IC3			
Country	**Complaints**	**Country**	**Complaints**
United Kingdom	102,692	**Mexico**	1,116
Canada	6,951	**South Africa**	1,075
India	4,189	**Pakistan**	979
France	2,223	**Indonesia**	895
Philippines	1,790	**Italy**	761
Australia	1,533	**Sweden**	732
Germany	1,524	**China**	651
Japan	1,492	**Turkey**	649
Brazil	1,472	**Spain**	639
Honduras	1,352	**Netherlands**	598

Transactional information provided in IC3 complaints also helps identify where funds are going when victims are directed to send funds overseas.

[14]

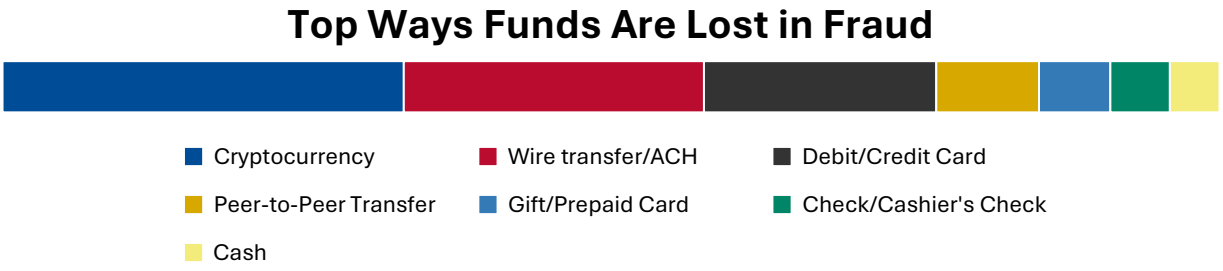


[13] Accessibility description: Charts list the top 20 countries by number of total complaints submitted to IC3, aside from the U.S. Please see Appendix C for more information regarding IC3 data.

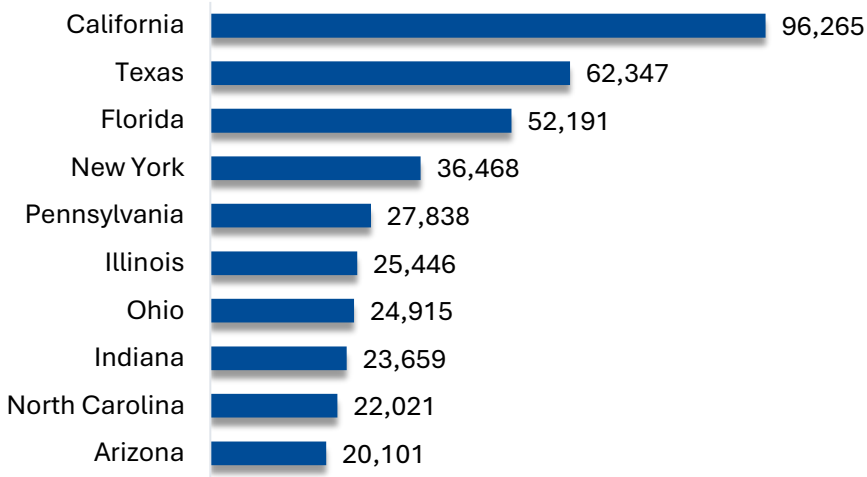
[14] Accessibility description: Chart shows the countries with the highest number of reported fraudulent wire transactions in 2024.

TOP REPORTED TRANSACTION TYPES[15]

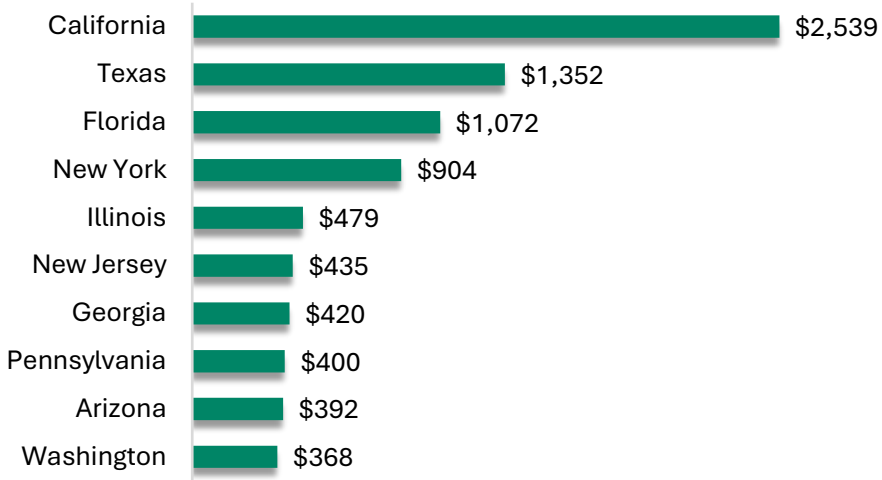
Transaction information provided in IC3 complaints helps FBI understand how victims are losing funds to fraud and assists the Recovery Asset Team Financial Fraud Kill Chain process when complaints are filed as quickly as possible. This chart identifies the top ways complainants reported financial loss in fraud.



TOP 10 STATES BY NUMBER OF COMPLAINTS[16]



TOP 10 STATES BY LOSS (IN MILLIONS)[17]



[15] Accessibility description: Chart depicts the top reported transaction types: Cryptocurrency, Wire transfer/ACH, Debit/Credit Card, Peer-to-Peer, Check/Cashier's Check, Gift/Prepaid Card, and Cash.
[16] Accessibility description: Chart depicts the top 10 states based on number of complaints. These include California, Texas, Florida, New York, Pennsylvania, Illinois, Ohio, Indiana, North Carolina, and Arizona. Please see Appendix C for more information regarding IC3 data.
[17] Accessibility description: Chart depicts the top 10 states based on reported losses are labeled. These include California, Texas, Florida, New York, Illinois, New Jersey, Georgia, Pennsylvania, Arizona, and Washington. Please see Appendix C for more information regarding IC3 data.

THREE YEAR COMPLAINT COUNT COMPARISON

BY COMPLAINT COUNT

Crime Type	2024	2023	2022
Advanced Fee	7,097	8,045	11,264
Business Email Compromise	21,442	21,489	21,832
Botnet	587	540	568
Confidence Fraud/Romance	17,910	17,823	19,021
Credit Card/Check Fraud	12,876	13,718	22,985
Crimes Against Children	4,472	2,361	2,587
Data Breach	3,204	3,727	2,795
Employment	20,044	15,443	14,946
Extortion	86,415	48,223	39,416
Government Impersonation	17,367	14,190	11,554
Harassment/Stalking	11,672	9,587	11,779
Identity Theft	21,403	19,778	27,922
Investment	47,919	39,570	30,529
IPR/Copyright and Counterfeit	1,583	1,498	2,183
Lottery/Sweepstakes/Inheritance	3,690	4,168	5,650
Malware	441	659	762
Non-Payment/Non-Delivery	49,572	50,523	51,679
Other	12,318	8,808	9,966
Overpayment	2,705	4,144	6,183
Personal Data Breach	64,882	55,851	58,859
Phishing/Spoofing	193,407	298,878	321,136
Ransomware	3,156	2,825	2,385
Real Estate	9,359	9,521	11,727
SIM Swap	982	1,075	2,026
Tech Support	36,002	37,560	32,538
Threats of Violence	1,360	1,697	2,224

THREE YEAR COMPLAINT LOSS COMPARISON

BY COMPLAINT LOSS

Crime Type	2024	2023	2022
Advanced Fee	$102,074,512	$134,516,577	$104,325,444
Business Email Compromise	$2,770,151,146	$2,946,830,270	$2,742,354,049
Botnet	$8,860,202	$22,422,708	$17,099,378
Confidence Fraud/Romance	$672,009,052	$652,544,805	$735,882,192
Credit Card/Check Fraud	$199,889,841	$173,627,614	264,148,905
Crimes Against Children	$519,424	$2,031,485	$577,464
Data Breach	$364,855,818	$534,397,222	$459,321,859
Employment	$264,223,271	$70,234,079	$52,204,269
Extortion	$143,185,736	$74,821,835	$54,335,128
Government Impersonation	$405,624,084	$394,050,518	$240,553,091
Harassment/Stalking	$10,611,223	$9,677,332	$5,621,402
Identity Theft	$174,354,745	$126,203,809	189,205,793
Investment	$6,570,639,864	$4,570,275,683	$3,311,742,206
IPR/Copyright and Counterfeit	$8,715,512	$7,555,329	$4,591,177
Lottery/Sweepstakes/Inheritance	$102,212,250	$94,502,836	$83,602,376
Malware	$1,365,945	$1,213,317	$9,326,482
Non-Payment/Non-Delivery	$785,436,888	$309,648,416	$281,770,073
Other	$280,278,325	$240,053,059	$117,686,789
Overpayment	$21,452,521	$27,955,195	$38,335,772
Personal Data Breach	$1,453,296,303	$744,219,879	$742,438,136
Phishing/Spoofing	$70,013,036	$18,728,550	$160,015,411
Ransomware	$12,473,156	$59,641,384	$34,353,237
Real Estate	$173,586,820	$145,243,348	$396,932,821
SIM Swap	$25,983,946	$48,798,103	$72,652,571
Tech Support	$1,464,755,976	$924,512,658	$806,551,993
Threats of Violence	$1,842,186	$13,531,178	$4,972,099

OVERALL STATE STATISTICS

COMPLAINTS BY STATE*

Rank	State	Complaints	Rank	State	Complaints
1	**California**	96,265	30	**Alaska**	6,770
2	**Texas**	62,347	31	**Louisiana**	6,455
3	**Florida**	52,191	32	**Kentucky**	6,165
4	**New York**	36,468	33	**Connecticut**	5,695
5	**Pennsylvania**	27,838	34	**Kansas**	4,797
6	**Illinois**	25,446	35	**Arkansas**	4,240
7	**Ohio**	24,915	36	**New Mexico**	3,884
8	**Indiana**	23,659	37	**District of Columbia**	3,856
9	**North Carolina**	22,021	38	**Idaho**	3,081
10	**Arizona**	20,101	39	**Mississippi**	3,068
11	**Georgia**	19,797	40	**Delaware**	2,806
12	**Washington**	18,009	41	**Hawaii**	2,603
13	**Virginia**	17,466	42	**Nebraska**	2,603
14	**Michigan**	16,302	43	**West Virginia**	2,594
15	**New Jersey**	15,701	44	**New Hampshire**	2,340
16	**Maryland**	14,996	45	**Puerto Rico**	2,241
17	**Colorado**	14,848	46	**Maine**	2,137
18	**Massachusetts**	14,254	47	**Montana**	1,854
19	**Tennessee**	11,411	48	**Rhode Island**	1,642
20	**Nevada**	10,716	49	**Wyoming**	1,377
21	**Missouri**	10,028	50	**South Dakota**	1,298
22	**South Carolina**	9,661	51	**Vermont**	937
23	**Wisconsin**	9,619	52	**North Dakota**	885
24	**Minnesota**	9,264	53	**U.S. Minor Outlying Islands**	170
25	**Oregon**	9,011	54	**Guam**	96
26	**Alabama**	7,840	55	**American Samoa**	91
27	**Oklahoma**	7,479	56	**Virgin Islands, U.S.**	87
28	**Iowa**	7,193	57	**Northern Mariana Islands**	21
29	**Utah**	6,877			

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

OVERALL STATE STATISTICS *CONTINUED*

LOSSES BY STATE*

Rank	State	Loss	Rank	State	Loss
1	California	$2,539,041,635	30	Alabama	$103,771,880
2	Texas	$1,351,598,183	31	Puerto Rico	$91,363,707
3	Florida	$1,071,909,632	32	Louisiana	$87,411,457
4	New York	$903,975,003	33	Kansas	$80,300,908
5	Illinois	$479,054,271	34	New Mexico	$76,621,670
6	New Jersey	$434,856,424	35	Kentucky	$73,919,940
7	Georgia	$420,454,472	36	Iowa	$72,860,333
8	Pennsylvania	$400,082,312	37	Mississippi	$65,613,936
9	Arizona	$392,441,717	38	Idaho	$63,035,342
10	Washington	$368,203,209	39	Hawaii	$55,180,901
11	Massachusetts	$338,872,378	40	New Hampshire	$52,811,455
12	North Carolina	$324,287,947	41	Arkansas	$51,714,039
13	Virginia	$317,406,595	42	Nebraska	$46,730,894
14	District of Columbia	$291,531,458	43	Wyoming	$43,502,744
15	Ohio	$278,038,028	44	Delaware	$37,611,598
16	Nevada	$268,769,310	45	Montana	$31,603,407
17	Colorado	$243,517,403	46	Maine	$31,455,797
18	Michigan	$241,737,979	47	Alaska	$26,296,803
19	Maryland	$238,976,904	48	South Dakota	$24,957,446
20	Minnesota	$203,352,530	49	West Virginia	$24,196,661
21	Tennessee	$190,271,310	50	Rhode Island	$23,597,036
22	Missouri	$183,751,987	51	North Dakota	$21,831,953
23	Wisconsin	$169,942,495	52	Vermont	$11,285,112
24	South Carolina	$146,468,765	53	Guam	$2,532,544
25	Oregon	$144,160,344	54	Virgin Islands, U.S.	$1,441,830
26	Connecticut	$143,884,002	55	U.S. Minor Outlying Islands	$1,107,380
27	Utah	$129,414,310	56	American Samoa	$195,182
28	Indiana	$125,093,323	57	Northern Mariana Islands	$121,874
29	Oklahoma	$113,724,886			

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

OVERALL STATE STATISTICS *CONTINUED*

COMPLAINTS PER 100K CITIZENS*

Rank	State	Count	Rank	State	Count
1	Alaska	914.7	27	Georgia	177.1
2	District of Columbia	549.1	28	South Carolina	176.3
3	Indiana	341.7	29	New Hampshire	166.1
4	Nevada	328.0	30	New Jersey	165.3
5	Delaware	266.8	31	Montana	163.0
6	Arizona	265.1	32	Kansas	161.5
7	Colorado	249.2	33	Wisconsin	161.4
8	California	244.1	34	Michigan	160.8
9	Maryland	239.4	35	Missouri	160.6
10	Wyoming	234.3	36	Minnesota	159.9
11	Washington	226.3	37	Tennessee	157.9
12	Florida	223.3	38	Connecticut	155.0
13	Iowa	221.9	39	Idaho	153.9
14	Pennsylvania	212.8	40	Maine	152.1
15	Oregon	210.9	41	Alabama	152.0
16	Ohio	209.7	42	Rhode Island	147.6
17	Illinois	200.2	43	West Virginia	146.6
18	Massachusetts	199.7	44	Vermont	144.5
19	North Carolina	199.4	45	Louisiana	140.4
20	Texas	199.3	46	South Dakota	140.4
21	Virginia	198.2	47	Arkansas	137.3
22	Utah	196.3	48	Kentucky	134.4
23	New York	183.6	49	Nebraska	129.8
24	Oklahoma	182.6	50	North Dakota	111.1
25	New Mexico	182.3	51	Mississippi	104.2
26	Hawaii	180.0	52	Puerto Rico	70.0

* Note: This information is based on the estimated 2024 Census estimated data and the total number of complaints from each state, the District of Columbia, and Puerto Rico for which the complainant provided state information. Please see Appendix C for more information regarding IC3 data. https://www.census.gov/data/tables/time-series/demo/popest/2020s-state-total.html#v2024

OVERALL STATE STATISTICS *CONTINUED*

LOSSES PER 100K CITIZENS*

Rank	State	Loss	Rank	State	Loss
1	**District of Columbia**	$41,513,914	27	**Pennsylvania**	$3,059,025
2	**Nevada**	$8,225,617	28	**Missouri**	$2,942,166
3	**Wyoming**	$7,403,235	29	**North Carolina**	$2,935,789
4	**California**	$6,439,159	30	**Puerto Rico**	$2,852,179
5	**Arizona**	$5,175,704	31	**Wisconsin**	$2,850,918
6	**Massachusetts**	$4,748,658	32	**Montana**	$2,778,974
7	**Washington**	$4,626,726	33	**Oklahoma**	$2,776,898
8	**Florida**	$4,586,256	34	**North Dakota**	$2,740,752
9	**New Jersey**	$4,577,026	35	**Kansas**	$2,703,183
10	**New York**	$4,550,077	36	**South Dakota**	$2,699,068
11	**Texas**	$4,319,470	37	**South Carolina**	$2,673,358
12	**Colorado**	$4,087,582	38	**Tennessee**	$2,632,511
13	**Connecticut**	$3,915,137	39	**Michigan**	$2,383,896
14	**Hawaii**	$3,815,721	40	**Ohio**	$2,339,737
15	**Maryland**	$3,815,560	41	**Nebraska**	$2,330,178
16	**Illinois**	$3,769,066	42	**Iowa**	$2,247,743
17	**Georgia**	$3,760,478	43	**Maine**	$2,238,828
18	**New Hampshire**	$3,748,066	44	**Mississippi**	$2,229,457
19	**Utah**	$3,693,739	45	**Rhode Island**	$2,121,448
20	**Virginia**	$3,602,310	46	**Alabama**	$2,011,980
21	**New Mexico**	$3,596,829	47	**Louisiana**	$1,901,183
22	**Delaware**	$3,575,529	48	**Indiana**	$1,806,591
23	**Alaska**	$3,552,983	49	**Vermont**	$1,740,206
24	**Minnesota**	$3,510,223	50	**Arkansas**	$1,674,485
25	**Oregon**	$3,374,247	51	**Kentucky**	$1,611,028
26	**Idaho**	$3,149,218	52	**West Virginia**	$1,367,059

* Note: This information is based on the estimated 2024 Census estimated data and the total number of complaints from each state, the District of Columbia, and Puerto Rico for which the complainant provided state information. Please see Appendix C for more information regarding IC3 data. https://www.census.gov/data/tables/time-series/demo/popest/2020s-state-total.html#v2024

CRIME TYPES BY AGE GROUPS

COUNTS	UNDER 20	20 - 29	30 – 39	40 – 49	50 - 59
Advanced Fee	220	971	1,102	968	1,009
Business Email Compromise	90	800	2,058	2,934	3,047
Botnet	74	99	79	55	42
Confidence/Romance	272	1,219	1,814	2,056	2,365
Credit Card/Check Fraud	295	1,206	1,690	1,641	1,642
Crimes Against Children	1,367	140	73	58	28
Data Breach	33	147	358	523	402
Employment	604	3,674	2,916	2,003	1,516
Extortion	6,540	13,811	6,180	4,305	3,620
Government Impersonation	161	1,462	1,894	1,818	1,711
Harassment/Stalking	548	1,667	1,998	1,619	990
Identity Theft	288	1,922	3,550	3,163	2,688
Investment	399	3,453	6,822	6,873	5,797
IPR/Copyright and Counterfeit	24	146	216	198	168
Lottery/Sweepstakes/ Inheritance	31	168	298	343	708
Malware	47	86	113	89	66
Non-Payment/ Non-Delivery	1,691	7,644	8,436	7,466	5,848
Other	318	883	1,375	1,187	909
Overpayment	314	776	507	456	449
Personal Data Breach	1,335	6,312	10,756	9,870	7,008
Phishing/Spoofing	203	1,088	1,532	1,701	2,060
Ransomware	12	62	120	211	253
Real Estate	150	1,749	1,407	1,088	1,011
SIM Swap	7	58	185	213	172
Spoofing	127	615	955	902	1,045
Tech Support	279	1,928	2,537	2,794	3,584
Threats of Violence	118	254	326	249	168
Cryptocurrency	858	6,277	10,885	10,338	8,953

* 60+ crime type information is available in the 2024 IC3 Elder Fraud Report.

CRIME TYPES BY AGE GROUPS

LOSSES	UNDER 20	20 - 29	30 – 39	40 – 49	50 - 59
Advanced Fee	$289,546	$4,479,321	$9,638,362	$16,770,456	$12,970,490
Business Email Compromise	$11,067,986	$30,611,039	$207,186,022	$302,370,195	$361,651,832
Botnet	$60	$30,718	$2,691	$17,303,168	$2,001
Confidence/ Romance	$759,616	$11,016,901	$31,008,972	$46,027,157	$82,466,829
Credit Card/ Check Fraud	$687,043	$4,581,387	$9,861,167	$25,602,871	$21,660,432
Crimes Against Children	$95,862	$4,292	$45,366	$29,655	$499,469
Data Breach	$970,279	$3,251,108	$64,898,844	$43,983,317	$15,586,514
Employment	$1,971,457	$13,138,194	$15,419,807	$9,874,429	$10,102,359
Extortion	$2,080,479	$11,799,104	$8,777,342	$8,984,024	$7,784,643
Government Impersonation	$2,008,033	$34,354,239	$30,281,258	$20,880,418	$18,727,179
Harassment/ Stalking	$51,719	$676,809	$2,185,563	$2,699,273	$649,797
Identity Theft	$269,690	$4,522,239	$13,036,661	$17,427,975	$12,879,363
Investment	$13,571,240	$154,183,205	$540,646,646	$616,072,673	$871,842,750
IPR/Copyright and Counterfeit	$4,302	$61,107	$780,863	$1,662,760	$2,851,670
Lottery/Sweep-stakes/Inheritance	$28,558	$732,222	$2,118,356	$3,512,077	$3,856,993
Malware	$18,056	$43,693	$59,168	$202,908	$135,302
Non-Payment/ Non-Delivery	$1,578,742	$19,895,195	$40,383,092	$54,348,415	$49,535,571
Other	$1,366,980	$11,369,781	$22,380,525	$15,665,583	$16,411,270
Overpayment	$1,006,792	$2,055,986	$2,799,535	$2,737,512	$2,570,057
Personal Data Breach	$635,038	$20,180,645	$115,301,927	$224,444,555	$108,826,649
Phishing/Spoofing	$35,368	$1,229,413	$2,726,832	$2,612,598	$2,751,552
Ransomware	$0	$12,548	$37,660	$187,680	$517,222
Real Estate	$413,752	$4,784,750	$6,623,054	$9,331,733	$22,466,504
SIM Swap	$0	$800,617	$6,752,902	$6,250,788	$5,080,192
Spoofing	$780,878	$876,082	$2,624,922	$3,054,743	$3,665,661
Tech Support	$1,007,672	$14,019,656	$25,573,715	$48,163,755	$48,548,923
Threats of Violence	$4,181	$7,908	$6,063,974	$65,817	$331,395
Cryptocurrency	$14,745,598	$169,240,044	$695,761,773	$851,201,069	$904,569,789

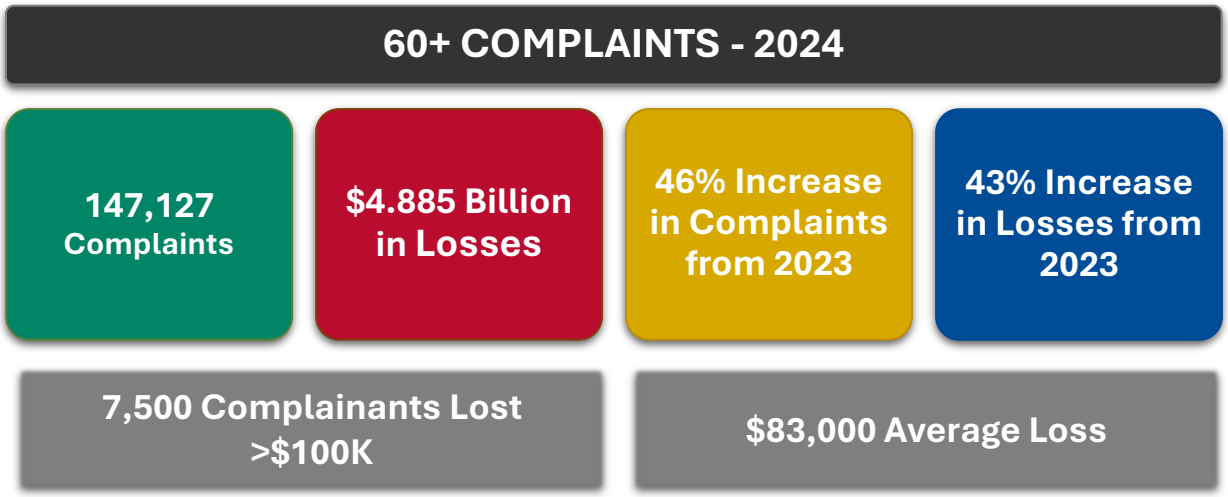
* 60+ crime type information is available in the 2024 IC3 Elder Fraud Report.

2024 Elder Fraud

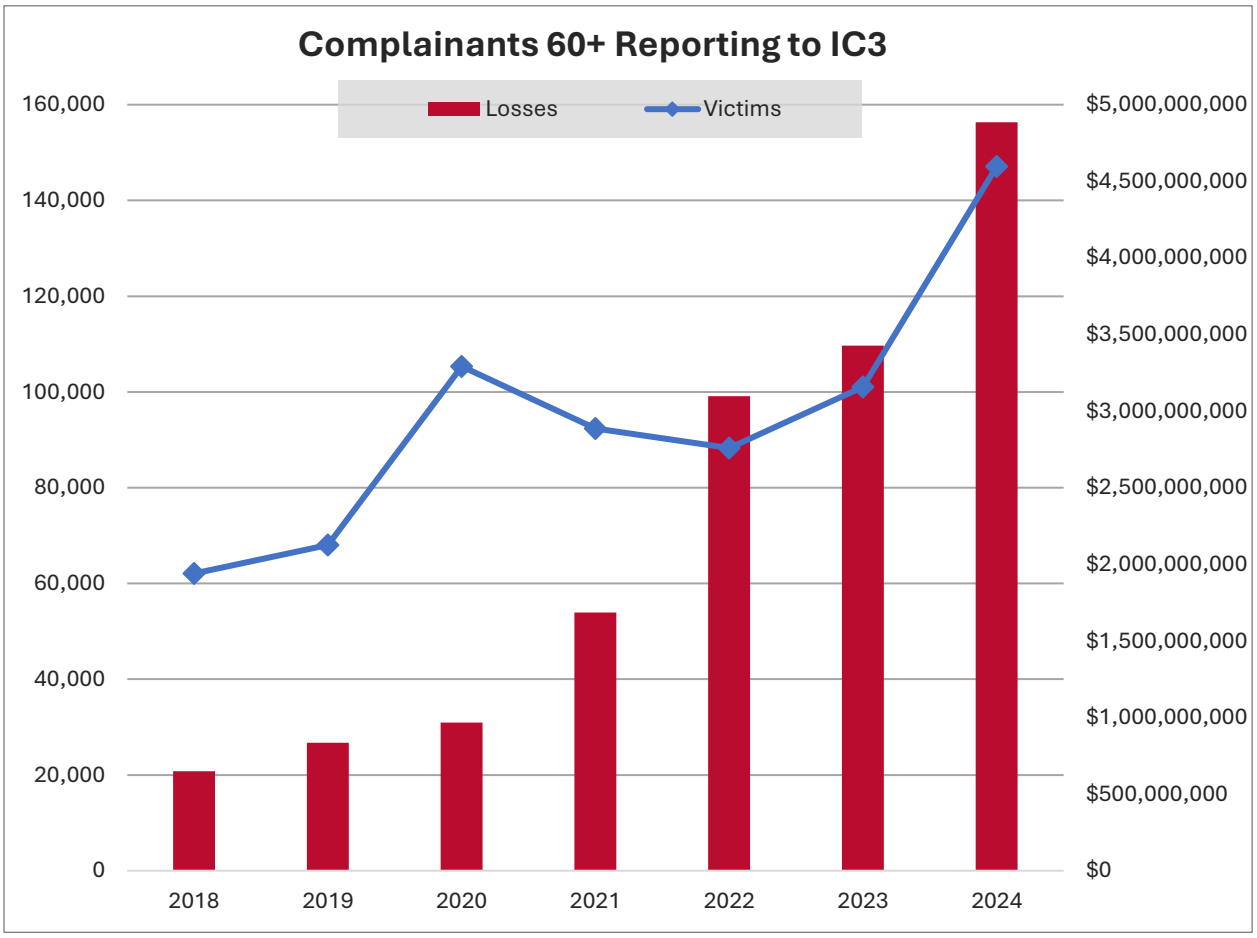
INTERNET CRIME COMPLAINT CENTER

COMPLAINTS FILED BY INDIVIDUALS 60+

[18]



[19]



[18] Charts describe count and loss trends for those 60+ from 2018 to 2024.
[19] Accessibility Description: Chart describes counts and losses for those reporting as 60+ from 2018 to 2024.

CRIME TYPES REPORTED BY 60+

COMPLAINANTS 60+			
Crime Type	Count	Crime Type	Count
Phishing/Spoofing	23,252	**Advanced Fee**	1,897
Tech Support	16,777	**Real Estate**	1,765
Extortion	12,618	**Lottery/Sweepstakes/Inheritance**	1,711
Personal Data Breach	9,827	**Harassment/Stalking**	696
Investment	9,448	**Overpayment**	527
Non-Payment/Non-Delivery	7,646	**Data Breach**	300
Confidence/Romance	7,626	**Ransomware**	208
Government Impersonation	4,521	**SIM Swap**	205
Identity Theft	4,064	**IPR/Copyright and Counterfeit**	163
Business Email Compromise*	3,300	**Threats of Violence**	111
Credit Card/Check Fraud	3,226	**Malware**	45
Other	2,017	**Crimes Against Children**	25
Employment	1,928	**Botnet**	23
Descriptor**			
Cryptocurrency	33,369		

*Regarding Business Email Compromise counts: A whole number is given to depict the overall complaint count and includes when a 60+ complainant may be reporting on behalf of a business or personally.

** This descriptor relates to the medium or tool used to facilitate the crime and are used by IC3 for tracking purposes only. It is available only after a crime type has been selected. Please see Appendix C for more information regarding IC3 data.

CRIME TYPES REPORTED BY 60+ *Continued*

COMPLAINANTS 60+ LOSSES			
Crime Type	**Loss**	**Crime Type**	**Loss**
Investment	$1,834,242,515	**Data Breach**	$28,546,213
Tech Support	$982,440,006	**Identity Theft**	$28,463,106
Confidence/Romance	$389,312,356	**Extortion**	$24,901,693
Business Email Compromise*	$385,001,099	**Phishing/Spoofing**	$20,202,521
Personal Data Breach	$254,187,196	**SIM Swap**	$6,342,329
Government Impersonation	$208,096,366	**Overpayment**	$5,900,921
Other	$111,300,637	**IPR/Copyright and Counterfeit**	$1,076,710
Non-Payment/Non-Delivery	$76,794,753	**Harassment/Stalking**	$713,693
Real Estate	$76,324,236	**Threats of Violence**	$300,488
Lottery/Sweepstakes/ Inheritance	$75,897,926	**Crimes Against Children**	$231,600
Advanced Fee	$41,622,868	**Malware**	$187,911
Employment	$37,882,347	**Ransomware****	$43,199
Credit Card/Check Fraud	$33,813,267	**Botnet**	$14,852
Descriptor***			
Cryptocurrency	$2,839,333,197		

* Regarding Business Email Compromise losses: A whole number is given to depict the overall complaint count and includes when a 60+ complainant may be reporting on behalf of a business or personally.

** 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 FBI, thereby creating an artificially low overall ransomware loss rate. Lastly, the number only represents what entities report to FBI via IC3 and does not account for the entity directly reporting to FBI field offices/agents.

*** This descriptor relates to the medium or tool used to facilitate the crime and used by IC3 for tracking purposes only. It is available only after a crime type has been selected. Please see Appendix C for more information regarding IC3 data.

THREE YEAR COMPARISON

60+ COMPLAINT COUNT			
Crime Type	2024	2023	2022
Advanced Fee	1,897	1,951	3,153
Business Email Compromise	3,300	3,080	3,938
Botnet	23	17	33
Confidence Fraud/Romance	7,626	6,740	7,166
Credit Card/Check Fraud	3,226	3,182	4,956
Crimes Against Children	25	26	84
Data Breach	300	336	333
Employment	1,928	1,079	1,286
Extortion	12,618	5,396	4,285
Government Impersonation	4,521	3,517	3,425
Harassment/Stalking	696	568	754
IPR/Copyright and Counterfeit	163	152	235
Identity Theft	4,064	3,010	4,825
Investment	9,448	6,443	4,661
Lottery/Sweepstakes/Inheritance	1,711	1,771	2,388
Malware	45	67	125
Non-Payment/Non-Delivery	7,646	6,693	7,985
Other	2,017	1,447	2,016
Overpayment	527	698	1,183
Personal Data Breach	9,827	7,333	7,849
Phishing/Spoofing	23,252	2,856	8,369
Ransomware	208	175	215
Real Estate	1,765	1,498	1,862
SIM Swap	205	174	301
Tech Support	16,777	17,696	17,810
Threats of Violence	111	115	166
Cryptocurrency	33,369	16,968	9,991

THREE YEAR COMPARISON, *Continued*

60+ COMPLAINT LOSSES			
Crime Type	2024	2023	2022
Advanced Fee	$41,622,868	$67,923,263	$49,322,099
Business Email Compromise	$385,001,099	$382,372,731	$477,342,728
Botnet	$14,852	$23,142	$120,621
Confidence Fraud/Romance	$389,312,356	$356,888,968	$419,768,142
Credit Card/Check Fraud	$33,813,267	$37,862,023	$61,649,198
Crimes Against Children	$231,600	$1,159,939	$48,373
Data Breach	$28,546,213	$23,913,130	$17,681,749
Employment	$37,882,347	$6,835,684	$6,403,021
Extortion	$24,901,693	$23,093,451	$15,555,047
Government Impersonation	$208,096,366	$179,646,103	$136,500,338
Harassment/Stalking	$713,693	$1,930,347	$254,659
IPR/Copyright and Counterfeit	$1,076,710	$183,169	$203,140
Identity Theft	$28,463,106	$34,551,900	$42,653,578
Investment	$1,834,242,515	$1,243,010,600	$990,235,119
Lottery/Sweepstakes/Inheritance	$75,897,926	$67,396,206	$69,845,106
Malware	$187,911	$261,144	$1,851,421
Non-Payment/Non-Delivery	$76,794,753	$59,018,965	$51,531,615
Other	$111,300,637	$72,707,042	$31,410,237
Overpayment	$5,900,921	$7,496,049	$10,977,231
Personal Data Breach	$254,187,196	$109,724,027	$127,736,607
Phishing/Spoofing	$20,202,521	$3,355,436	$36,715,205
Ransomware	$43,199	$635,548	$210,052
Real Estate	$76,324,236	$65,634,851	$135,239,020
SIM Swap	$6,342,329	$15,148,072	$19,515,629
Tech Support	$982,440,006	$589,759,770	$587,831,698
Threats of Violence	$300,488	$5,128,768	$376,458
Cryptocurrency	$2,839,333,197	$1,653,484,444	$1,088,330,051

OVERALL STATE STATISTICS

COUNTS BY STATE FROM COMPLAINTS FILED BY INDIVIDUALS 60+*

Rank	State	Count	Rank	State	Count
1	**California**	18,091	30	**Kentucky**	1,336
2	**Florida**	11,902	31	**Connecticut**	1,209
3	**Texas**	9,473	32	**New Mexico**	1,150
4	**Arizona**	6,683	33	**Kansas**	1,129
5	**Pennsylvania**	6,353	34	**Arkansas**	1,063
6	**New York**	6,225	35	**Iowa**	803
7	**Illinois**	6,064	36	**Idaho**	775
8	**Ohio**	5,388	37	**Hawaii**	647
9	**Indiana**	5,324	38	**New Hampshire**	633
10	**North Carolina**	5,031	39	**Maine**	608
11	**Virginia**	3,841	40	**Mississippi**	604
12	**Washington**	3,692	41	**West Virginia**	594
13	**Georgia**	3,622	42	**Nebraska**	551
14	**Maryland**	3,231	43	**Delaware**	514
15	**Massachusetts**	3,224	44	**Alaska**	466
16	**Michigan**	3,148	45	**Montana**	438
17	**Colorado**	3,128	46	**Rhode Island**	324
18	**New Jersey**	2,918	47	**Puerto Rico**	285
19	**Tennessee**	2,543	48	**District of Columbia**	267
20	**Nevada**	2,299	49	**Wyoming**	267
21	**South Carolina**	2,293	50	**South Dakota**	259
22	**Oregon**	2,288	51	**Vermont**	243
23	**Missouri**	2,199	52	**North Dakota**	174
24	**Oklahoma**	1,858	53	**U.S. Minor Outlying Islands**	39
25	**Minnesota**	1,836	54	**Guam**	20
26	**Wisconsin**	1,785	55	**Virgin Islands, U.S.**	17
27	**Utah**	1,762	56	**Northern Mariana Islands**	2
28	**Alabama**	1,567	57	**American Samoa**	1
29	**Louisiana**	1,372			

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

OVERALL STATE STATISTICS, *Continued*

LOSSES BY STATE FROM COMPLAINTS FILED BY INDIVIDUALS 60+*

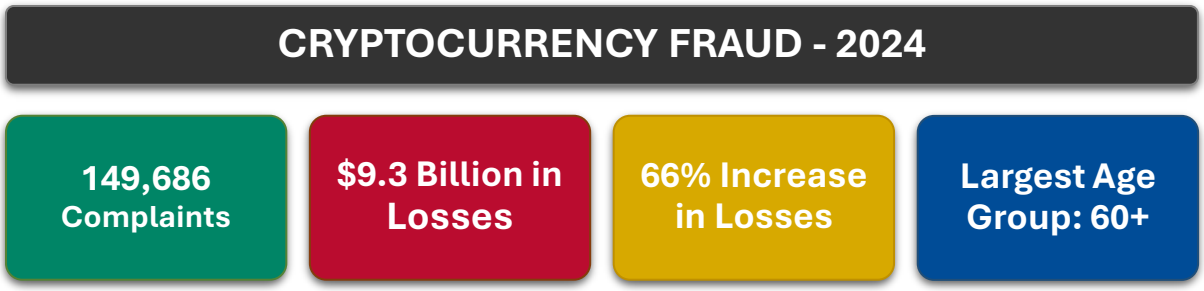
Rank	State	Loss	Rank	State	Loss
1	**California**	$832,710,048	30	**Iowa**	$34,991,114
2	**Texas**	$489,790,386	31	**Alabama**	$33,200,314
3	**Florida**	$388,436,198	32	**Connecticut**	$30,918,559
4	**New York**	$257,658,301	33	**New Mexico**	$30,034,919
5	**District of**	$251,454,544	34	**Mississippi**	$28,870,444
6	**Arizona**	$190,686,835	35	**Arkansas**	$27,253,501
7	**Georgia**	$174,744,201	36	**Kentucky**	$26,139,251
8	**Pennsylvania**	$151,096,514	37	**Kansas**	$23,511,153
9	**Illinois**	$133,794,241	38	**Nebraska**	$21,414,248
10	**New Jersey**	$133,397,512	39	**Puerto Rico**	$20,183,422
11	**Washington**	$107,052,160	40	**Hawaii**	$18,851,052
12	**Virginia**	$106,575,141	41	**Idaho**	$18,663,392
13	**Massachusetts**	$99,804,762	42	**New Hampshire**	$15,840,854
14	**Ohio**	$95,441,773	43	**Maine**	$12,980,616
15	**Michigan**	$92,378,793	44	**Delaware**	$12,293,619
16	**North Carolina**	$87,449,567	45	**Montana**	$12,056,193
17	**Nevada**	$81,400,930	46	**South Dakota**	$8,975,829
18	**Maryland**	$80,128,654	47	**Wyoming**	$8,648,675
19	**Colorado**	$74,760,501	48	**Alaska**	$8,173,395
20	**Missouri**	$63,530,750	49	**Rhode Island**	$6,309,411
21	**Tennessee**	$61,882,884	50	**West Virginia**	$5,790,489
22	**South Carolina**	$58,581,997	51	**North Dakota**	$5,781,845
23	**Minnesota**	$52,262,721	52	**Vermont**	$4,177,269
24	**Wisconsin**	$50,525,457	53	**U.S. Minor Outlying**	$670,314
25	**Oklahoma**	$50,203,394	54	**Guam**	$592,965
26	**Oregon**	$48,116,839	55	**Virgin Islands, U.S.**	$163,884
27	**Utah**	$44,155,961	56	**American Samoa**	$3,000
28	**Louisiana**	$37,512,993	57	**Northern Mariana Islands**	$120
29	**Indiana**	$37,209,947			

* Note: This information is based on the total losses in each state, American Territory, and the District of Columbia for which the complainant provided state information. Please see Appendix C for more information regarding IC3 data.

2024 Cryptocurrency Fraud

INTERNET CRIME COMPLAINT CENTER

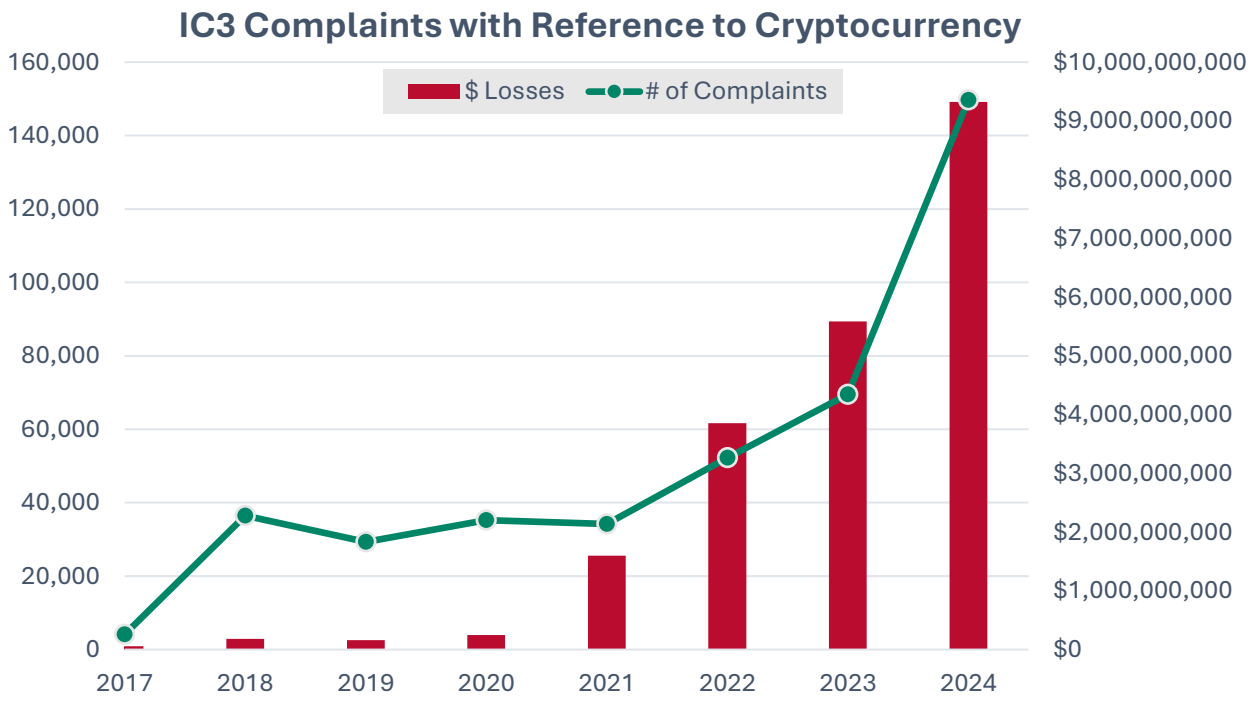
2024 IC3 CRYPTOCURRENCY FRAUD



[20]

COMPLAINTS REFERENCING CRYPTOCURRENCY		
AGE RANGE[21]	**COUNT**	**LOSS**
Under 20	1,819	$7,778,157
20 - 29	13,591	$370,443,345
30 - 39	22,218	$1,006,382,458
40 - 49	22,555	$1,462,040,974
50 - 59	19,317	$1,184,912,854
Over 60	33,369	$2,839,333,197

[22]



[20] Accessibility description: Chart outlines cryptocurrency complaints in 2024: 149,686 complaints; $9.3 billion in losses; 66% increase in loss; largest age group to report is 60+.

[21] Not all complaints include an associated age range—those without this information are excluded from this table. Please see Appendix C for more information regarding IC3 data.

[22] Chart outlines the number of cryptocurrency related complaints from 2017 to 2024.

CRYPTOCURRENCY in FRAUD TRENDS

Cryptocurrency Investment

41,557 Complaints; $5.8 Billion in Losses

29% Increase in Complaints from 2023
47% Increase in Losses from 2023

The FBI Warns of a Spike in Cryptocurrency Investment Schemes

CRYPTO INVESTMENT FRAUD by AGE GROUP

Age Group	Count	Losses
Under 20	303	$3,307,216
20 - 29	2,906	$273,447,400
30 - 39	6,217	$373,696,736
40 - 49	7,145	$1,053,964,645
50 - 59	6,364	$811,298,119
Over 60	8,043	$1,600,353,509

Cryptocurrency ATMs/Kiosks

10,956 Complaints; $246.7 Million in Losses

99% Increase in Complaints from 2023
31% Increase in Losses from 2023

The FBI Warns of Fraudulent Schemes Leveraging Cryptocurrency ATMs and QR Codes to Facilitate Payment

REPORTS of CRYPTO ATM/KIOSK USE by AGE GROUP

Age Group	Count	Losses
Under 20	7	$51,913
20 - 29	280	$3,739,620
30 - 39	361	$4,241,387
40 - 49	319	$3,621,774
50 – 59	349	$5,523,230
Over 60	2,674	$107,206,251

CRIME TYPES MOST ASSOCIATED WITH CRYPTO ATM USE

	Count	Losses		Count	Losses
Extortion	4,189	$5,601,953	**Government Impersonation**	1,786	$44,587,335
Tech Support	3,037	$107,429,709	**Investment**	606	$38,090,269

Extortion/Sextortion

54,936 Complaints; $33.5 Million in Losses

59% Increase in Complaints from 2023
9% Increase in Losses from 2023

Malicious Actors Manipulating Photos and Videos to Create Explicit Content and Sextortion Schemes

EXTORTION / SEXTORTION by AGE GROUP

Age Group	Count	Losses
Under 20	3,806	$1,006,975
20 - 29	13,302	$5,471,516
30 - 39	9,204	$5,473,072
40 - 49	6,794	$3,726,438
50 - 59	4,940	$2,899,089
Over 60	5,903	$7,821,886

CRIME TYPES WITH CRYPTOCURRENCY NEXUS

COMPLAINTS			
Crime Type	Count	Crime Type	Count
Extortion	47,054	**Identity Theft**	527
Investment	41,557	**Credit Card/Check Fraud**	389
Personal Data Breach	11,644	**Ransomware**	389
Tech Support	11,129	**Lottery/Sweepstakes/Inheritance**	329
Employment	6,533	**Business Email Compromise**	256
Phishing/Spoofing	3,938	**Real Estate**	256
Confidence/Romance	3,811	**SIM Swap**	215
Government Impersonation	3,585	**Harassment/Stalking**	211
Non-Payment/Non-Delivery	2,492	**Overpayment**	186
Advanced Fee	1,537	**Malware**	53
Other	1,315	**Botnet**	44
Data Breach	846	**Crimes Against Children**	42

Descriptor*	
Cryptocurrency	149,686

* This descriptor relates to the medium or tool used to facilitate the crime and are used by IC3 for tracking purposes only. It is available only after a crime type has been selected. Please see Appendix C for more information regarding IC3 data.

CRIME TYPES WITH CRYPTOCURRENCY NEXUS *Continued*

LOSSES			
Crime Type	Loss	Crime Type	Loss
Investment	$5,819,531,069	**SIM Swap**	$28,463,106
Personal Data Breach	$1,120,793,009	**Credit Card/Check Fraud**	$24,901,693
Tech Support	$961,998,313	**Identity Theft**	$20,202,521
Confidence/Romance	$237,151,771	**Lottery/Sweepstakes/ Inheritance**	$6,342,329
Employment	$197,224,612	**Real Estate**	$5,900,921
Data Breach	$167,874,424	**Ransomware***	$1,076,710
Government Impersonation	$146,057,054	**Botnet**	$713,693
Extortion	$96,072,767	**Overpayment**	$300,488
Business Email Compromise	$63,882,699	**Harassment/Stalking**	$231,600
Other	$63,516,319	**Malware**	$187,911
Non-Payment/Non-Delivery	$55,139,529	**IPR/Copyright and Counterfeit**	$43,199
Advanced Fee	$36,436,824	**Threats of Violence**	$289,288
Phishing/Spoofing	$28,546,213	**Crimes Against Children**	$19,174
Descriptor**			
Cryptocurrency	$9,322,335,911		

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

** This descriptor relates to the medium or tool used to facilitate the crime and are used by IC3 for tracking purposes only. It is available only after a crime type has been selected. Please see Appendix C for more information regarding IC3 data.

OVERALL STATE STATISTICS

CRYPTOCURRENCY COMPLAINTS BY STATE*

Rank	State	Count	Rank	State	Count
1	**California**	19,508	30	**Kentucky**	1,196
2	**Texas**	11,270	31	**Louisiana**	1,165
3	**Florida**	10,698	32	**New Mexico**	885
4	**New York**	8,053	33	**Kansas**	862
5	**Pennsylvania**	4,355	34	**Idaho**	835
6	**Illinois**	4,319	35	**Arkansas**	775
7	**New Jersey**	4,259	36	**Hawaii**	709
8	**Washington**	4,169	37	**Iowa**	668
9	**Arizona**	4,145	38	**Mississippi**	582
10	**Virginia**	4,016	39	**New Hampshire**	547
11	**North Carolina**	3,684	40	**Nebraska**	541
12	**Georgia**	3,533	41	**District of Columbia**	534
13	**Ohio**	3,371	42	**Alaska**	453
14	**Colorado**	3,218	43	**Maine**	429
15	**Maryland**	3,158	44	**Montana**	421
16	**Massachusetts**	3,015	45	**Delaware**	406
17	**Michigan**	3,009	46	**West Virginia**	406
18	**Tennessee**	2,354	47	**Rhode Island**	329
19	**Nevada**	2,153	48	**Puerto Rico**	278
20	**Oregon**	2,070	49	**South Dakota**	254
21	**Wisconsin**	1,973	50	**Wyoming**	250
22	**Missouri**	1,951	51	**Vermont**	207
23	**South Carolina**	1,944	52	**North Dakota**	184
24	**Indiana**	1,880	53	**U.S. Minor Outlying Islands**	28
25	**Minnesota**	1,852	54	**Guam**	15
26	**Utah**	1,658	55	**Virgin Islands, U.S.**	13
27	**Connecticut**	1,361	56	**American Samoa**	5
28	**Alabama**	1,313	57	**Northern Mariana Islands**	3
29	**Oklahoma**	1,208			

* 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 C for more information regarding IC3 data.

OVERALL STATE STATISTICS, *Continued*

CRYPTOCURRENCY LOSSES BY STATE*

Rank	State	Loss	Rank	State	Loss
1	**California**	$1,393,628,996	30	**Louisiana**	$49,306,020
2	**Texas**	$738,583,341	31	**Kansas**	$49,045,398
3	**Florida**	$584,746,970	32	**Indiana**	$48,009,883
4	**New York**	$375,087,857	33	**New Mexico**	$43,269,446
5	**Illinois**	$272,633,678	34	**Oklahoma**	$37,752,198
6	**District of Columbia**	$262,640,821	35	**Wyoming**	$36,386,737
7	**New Jersey**	$236,721,074	36	**Idaho**	$35,149,916
8	**Pennsylvania**	$218,642,276	37	**Kentucky**	$32,907,797
9	**Washington**	$204,694,032	38	**Hawaii**	$24,893,821
10	**Massachusetts**	$201,530,349	39	**Nebraska**	$23,094,744
11	**Georgia**	$197,647,537	40	**New Hampshire**	$22,699,416
12	**Nevada**	$185,521,892	41	**Arkansas**	$20,654,583
13	**Arizona**	$177,578,809	42	**Iowa**	$20,350,712
14	**North Carolina**	$174,411,615	43	**Delaware**	$19,973,180
15	**Virginia**	$158,769,093	44	**Maine**	$17,137,660
16	**Maryland**	$132,730,401	45	**Mississippi**	$14,505,794
17	**Colorado**	$130,631,488	46	**South Dakota**	$13,811,508
18	**Michigan**	$126,330,606	47	**Montana**	$12,900,561
19	**Ohio**	$123,379,667	48	**Rhode Island**	$12,556,877
20	**Missouri**	$93,029,140	49	**Alaska**	$11,780,664
21	**Minnesota**	$91,614,693	50	**North Dakota**	$7,700,246
22	**Tennessee**	$82,748,140	51	**West Virginia**	$7,686,156
23	**Puerto Rico**	$71,185,851	52	**Vermont**	$4,265,121
24	**Oregon**	$68,159,115	53	**U.S. Minor Outlying Islands**	$874,714
25	**Utah**	$68,133,250	54	**Guam**	$751,009
26	**Wisconsin**	$67,513,795	55	**Virgin Islands, U.S.**	$324,580
27	**South Carolina**	$60,529,485	56	**American Samoa**	$145,182
28	**Connecticut**	$59,749,544	57	**Northern Mariana Islands**	$16,946
29	**Alabama**	$51,273,598			

* 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 C for more information regarding IC3 data.

APPENDIX A: ABOUT IC3

Today's FBI is an intelligence-driven and threat focused national security organization with both intelligence and law enforcement responsibilities. FBI is 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, FBI leverages IC3 as a mechanism to gather intelligence on cybercrime so that we can provide the public and our many partners with information, services, support, training, and leadership to stay ahead of the threat.

Every day, IC3 receives thousands of complaints reporting a wide array of scams, many of them targeting our most vulnerable populations. The information submitted to 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 FBI to connect complaints, investigate reported crimes, track trends and threats, and, in some cases, even freeze stolen funds. Just as importantly, 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.

IC3 was established in May 2000 to receive complaints crossing the spectrum of cyber matters, to include cyber threats and cyber-enabled fraud in their many forms including ransomware, intrusions (hacking), extortion, international money laundering, investment fraud, and a growing list of crimes. As of publication, IC3 has received over 9 million complaints. 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.

To promote public awareness and as part of its prevention mission, 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 IC3.gov interface. Their efforts help IC3 and FBI better protect their fellow citizens.

Frauds and scams will continue to evolve, but many characteristics of these schemes remain the same even as new trends develop. Review previous IC3 Annual Reports and Public Service Announcements (PSAs) to further educate and protect yourself, as well as your family, friends, and community.

APPENDIX B: DEFINITIONS

Advanced Fee Fraud: 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 Fraud: 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 Fraud: An individual believes they are legitimately employed and loses money, or launders money/items during 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 to collect or extort money.

Harassment/Stalking: Repeated words, conduct, and/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 Fraud: 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.).

Intellectual Property Rights (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 Fraud: 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 Fraud: 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).

Other: Criminal or civil matters not currently designated as an IC3 crime type.

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 Fraud: 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 Fraud: 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 C: ADDITIONAL INFORMATION ABOUT IC3 DATA

- As appropriate, complaints are reviewed by IC3 analysts, who apply descriptive data, such as crime type and adjusted loss.
- Descriptive data for complaints, such as crime type or loss, is variable and can evolve based upon investigative or analytical proceedings. Statistics are an assessment taken at a point in time, which may change.
- Complainants are not required to provide an age range.
- Each complaint will only have one crime type.
- Complainant 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.

APPENDIX D: PUBLIC SERVICE ANNOUCEMENTS PUBLISHED

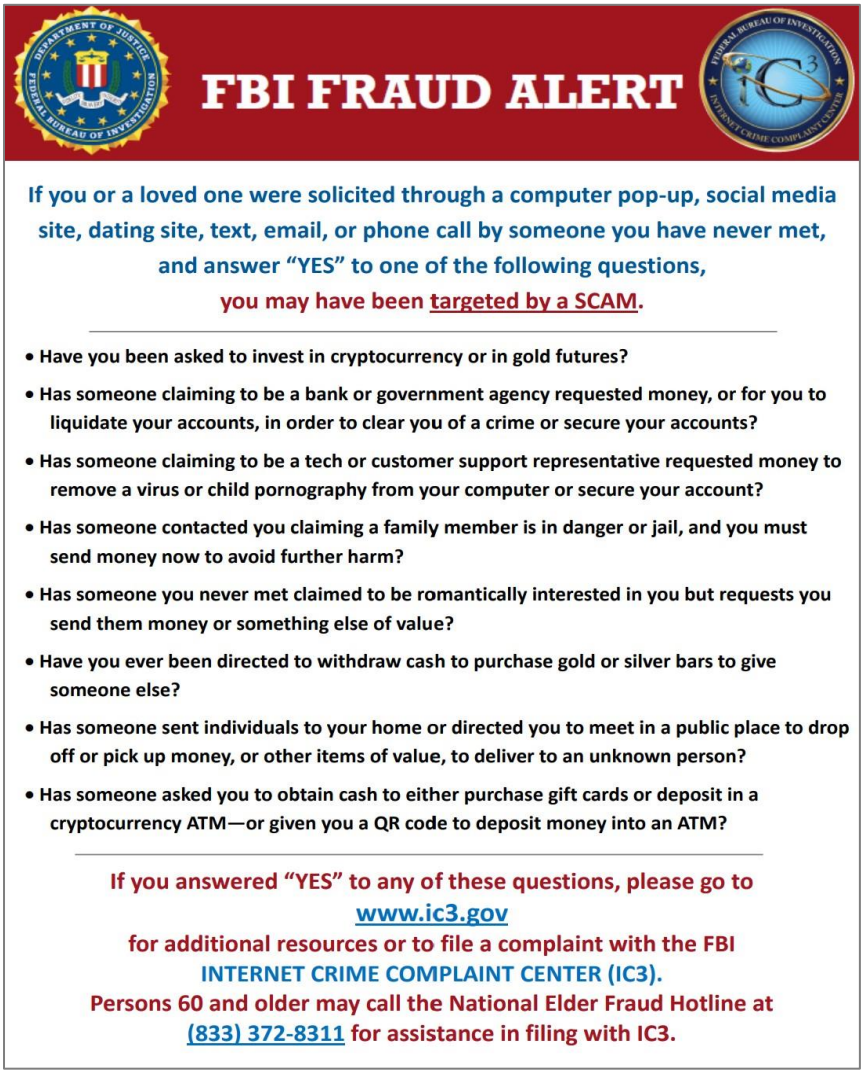
Title	Date
Chinese Police Imposters Incorporate Aggressive Tactics to Target U.S.-Based Chinese Community	1/3/2024
Malicious Actors Threaten U.S. Synagogues, Schools, Hospitals, and Other Institutions with Bomb Threats	1/12/2024
Scammers Use Couriers to Retrieve Cash and Precious Metals from Victims of Tech Support and Government Impersonation Scams	1/29/2024
IC3 Annual Report and Fraud Flyer	3/18/2024
Child Sexual Abuse Material Created by Generative AI and Similar Online Tools is Illegal	3/29/2024
Cyber Criminals Target Victims Using Social Engineering Techniques	4/11/2024
Smishing Scam Regarding Debt for Road Toll Services	4/12/2024
Alert on Cryptocurrency Money Services Businesses	4/25/2024
New Verification Schemes Target Users of Online Dating Platforms	4/26/2024
Foreign Terrorist Organizations and their Supporters Likely Heighten Threat Environment during 2024 Pride Month	5/10/2024
Democratic People's Republic of Korea Leverages U.S.-Based Individuals to Defraud U.S. Businesses and Generate Revenue	5/16/2024
Guidance on the 911 S5 Residential Proxy Service	5/29/2024
Scammers Defraud Individuals via Work-From-Home Scams	6/4/2024
Fictitious Law Firms Targeting Cryptocurrency Scam Victims Offering to Recover Funds	6/24/2024
Scammers Falsely Promise Significant Profit to Victims in Collectible Coin Scams	6/25/2024
DDoS Attacks: Could Hinder Access to Election Information, Would Not Prevent Voting	7/31/2024
FBI Warns of Scammers Impersonating Cryptocurrency Exchanges	8/1/2024
Safety Concern Related to Recent Trend in Financial Institution Customer Fraud Scheme	8/2/2024
Just So You Know: Ransomware Disruptions during Voting Periods Will Not Impact the Security and Resiliency of Vote Casting or Counting	8/15/2024
North Korea Aggressively Targeting Crypto Industry with Well-Disguised Social Engineering Attacks	9/3/2024
Business Email Compromise: The $55 Billion Scam	9/11/2024

Just So You Know: False Claims of Hacked Voter Information Likely Intended to Sow Distrust of U.S. Elections	9/12/2024
Anniversary of October 7, 2023, HAMAS Attacks May Motivate Individuals to Violence in the United States	10/4/2024
Counterfeit Check Scam Targets Law Firms Via Debt Collection Scheme	10/8/2024
Just So You Know: Foreign Threat Actors Likely to Use a Variety of Tactics to Develop and Spread Disinformation During 2024 U.S. General Election Cycle	10/18/2024
Scammers Exploit 2024 US General Election to Perpetrate Multiple Fraud Schemes	10/29/2024
Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud	12/3/2024

APPENDIX E: EDUCATIONAL MATERIALS PUBLISHED

Check – Call – Wait
Avoid falling to a BEC scam.

IC3 Fraud Flyer



Osseo Area Schools

1 Yr Board Calendar Meeting Topics – 2025-2026 School Year *(working draft)*

Draft March 18, 2025; updated September 9, 2025

* **indicates Student School Board Representatives in attendance to provide input**

Osseo Area Schools Proposed Topics: July-December 2025 Agenda/Calendar						
	July	**August**	**September**	**October**	**November**	**December**
District Policy				• **Policy Committee Mtg** (10/7/25)		• **Policy Committee Mtg** (12/9/25
Op Over-sight	**Regular Meeting** (7/22/25) • Consent agenda (teacher contracts) • Gifts to the district (brief meeting to act on required business)	**Work Session** (8/19/25) • Safety Management (portion of this agenda item to be closed to the public) • Naming of New Elementary • Board calendar review **Regular Mtg** (8/26/25) • Presentation: Logo and Signage • Superintendent's Report • Non-public contracts for Student Services • Contract approvals • First Reading of Policy (Series 200) • Negotiation Strat Mtg (closed)	**Work Session** (9/9/25)) • ~~Continue Committee Work~~ (to be rescheduled) • Monitoring Report A • Crest View Update • Board calendar review **Regular Mtg** (9/23/25) • Introduction of Student Board Representatives • Superintendent's Report • Preliminary Levy (action item with presentation) • Preliminary FY 2025 Financial Report (presentation) • General Liability Insurance Renewal • Negotiation Strat Mtg (closed)	**Work Session** (10/7/25) (Meeting location: Brooklyn Middle) • Student Stakeholder Survey* • Cyber Security • Instructional Leader presentation **Regular Mtg** (10/21/25) • AVID presentation • Student Board Representatives Report (to present summary of Student Stakeholder Survey discussion) • Superintendent's Report • Contract ratifications • Lobbyist contract approval • Negotiation Strategies Meeting (closed session) **Professional Development** (10/28/25) (Continue Committee Work)	**Work Session** (11/11/25) • Staff retention • Comprehensive Engagement and Civic Readiness (CECR), formerly World's Best Workforce, Results • LRFP Budget Parameters **Regular Mtg** (11/18/25) • Student Board Representatives Report • Superintendent's Report • FY25 Financial Audit Results presentation • Negotiation Strategies Meeting (closed session)	**Work Session (12/9/25)** • Legislative Platform • 500 Series policies * **Regular Mtg** (12/16/25) • Student Board Representatives Report (to present summary of 500 Series policies) • Superintendent's Report • Legislative Platform • Final Levy/Truth in Taxation • LTFM Update • 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)	**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)

(over)

*** indicates Student School Board Representatives in attendance to provide input**

Osseo Area Schools

DRAFT Proposed Topics: January-June 2026 Agenda/Calendar

	January	February	March	April	May	June
District Policy			• Policy Committee Meeting (3/10/26))			• Policy Committee Meeting (6/9/26)
Op Over-sight	**Organizational Meeting** (1/6/26) • 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** • Standards-based Grading Practices • xxx • xxx **School Board Professional Development** (1/13/26) • xxx **Regular Mtg** (1/20/26) • xxx • Negotiations Strategy Meeting (SM/closed session)	**Work Session** (2/10/26) • LRFP Budget Update • Standards-based Grading Practices* (with Student Board Reps) **Regular Mtg** (2/24/26) • Student Board Representatives Report (to present summary of Standards-based Grading Practices discussion) • FY26 Budget Adjustments • FY26 Capital Budget Approval • Contract ratifications • Negotiations Strategy Meeting (SM/closed session)	**Work Session** 3/10/26) • Somali community outreach • xx • xx **Regular Mtg** (3/17/26) • Student Board Representatives Report • Technology bid awards • E-rate bid awards • Contract ratifications • Negotiations Strategy Meeting (SM/closed session)	**Work Session** (4/7/26) • Vision Cards C & D • xx **Regular Mtg** (4/21/26) • Student Board Representatives Report • District Planning Advisory Council (DPAC) Recommendations • Insurance renewals • November 2026 election resolutions • Contract ratifications • Negotiations Strategy Meeting (SM/closed session)	**Work Session** (5/5/26) • xx • xx • xx • xx *School Board closed session following work session for purpose of supt. evaluation* **Regular Mtg** (5/19/26) • Retiree recognition • Student board rep recognition • ECMAC Recommendations • November 2026 election resolutions • Termination of probationary teachers • Contract ratifications • Negotiations Strategy Meeting (SM/closed session)	**Work Session** (6/9/26 • 2026-27 Budget • Legislative Update • Vision Cards B & E **Regular Mtg** (6/23/26) • 2026-27 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)				School board conduct superintendent evaluation (closed meeting, May); report out (summary) at July meeting	
Public Engage-ment						