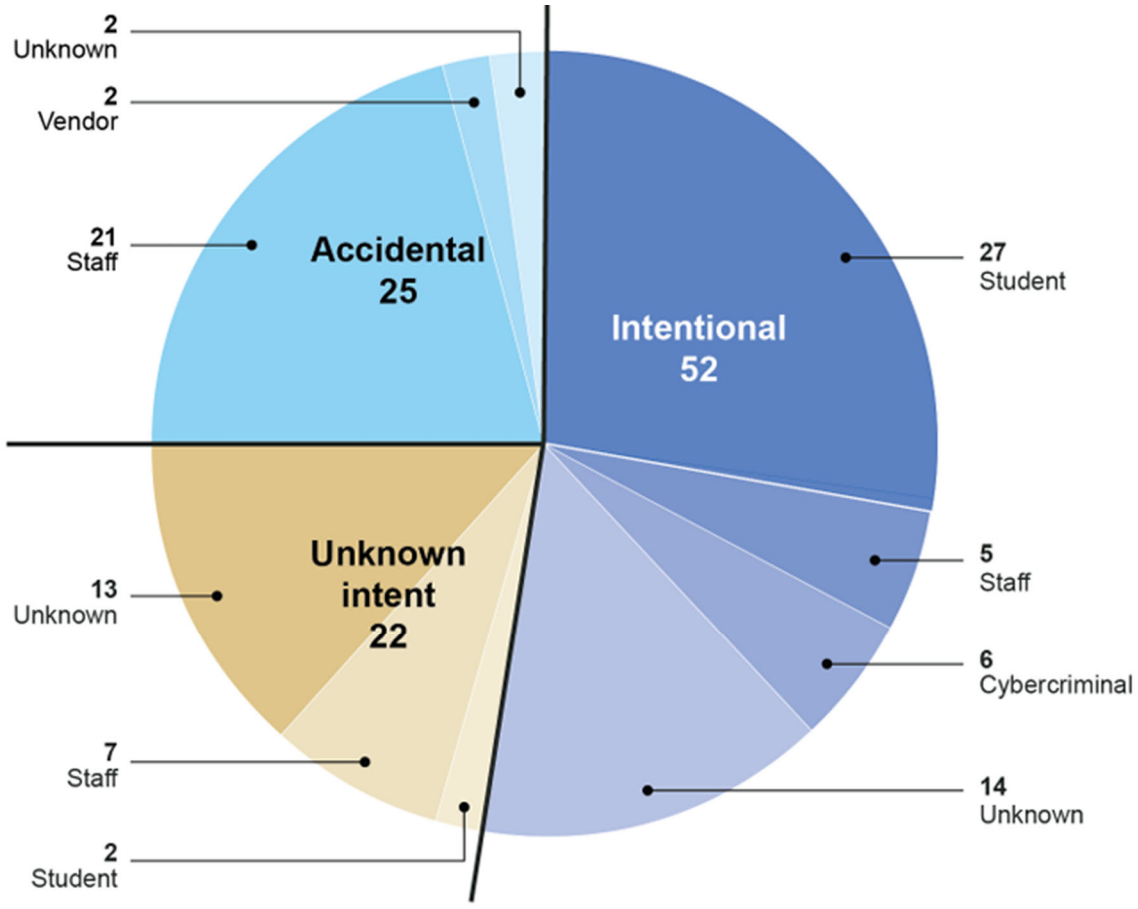
GEMA/HS Intelligence Unit

(U) THREAT ACTORS TARGETING STUDENT PII – JANUARY 2023

(U) *Why are Threat Actors Targeting Schools?*

Recent data trends have shown that school systems are being targeted by threat actors at a disproportionate rate compared to other agency types. The Personally Identifiable Information (PII) of employees and students at schools impacted by cyber-attacks has become a lucrative target for threat actors. PII that has been exfiltrated by threat actors is sold routinely on dark web forums and marketplaces. Social security numbers (SSN) are used to acquire credit and identification. PII is more valuable to a cyber-criminal when the owner is a juvenile because juveniles are less likely to notice its loss until they are old enough to access their SSN (e.g., purchasing a home, obtaining a passport, employment, etc.).

Figure 1: Reported Number of K-12 Cybersecurity Student Data Breaches by Actor and Intent, July 1, 2016-May 5, 2020, additional information from the United States Government Accountability Office can be found here.



Source: GAO analysis of K-12 Cybersecurity Resource Center data. | GAO-20-644

(U) *County Level Stats from 2022*

County level agencies within Georgia are being targeted by threat actors at an elevated rate compared to other agency types. Social engineering is an attack vector that allows more intrusive and disruptive attacks to happen further down the line, such as ransomware attacks. Most forms of cyber-attack will have the user's data as the end goal, either for exploitation or pivoting purposes resulting in a data breach. By looking at the data collected for incident types impacting Georgia, school systems are being impacted by cyber incidents. Out of the 14 county level incidents reported in 2022, 9 of those reports were from school systems.

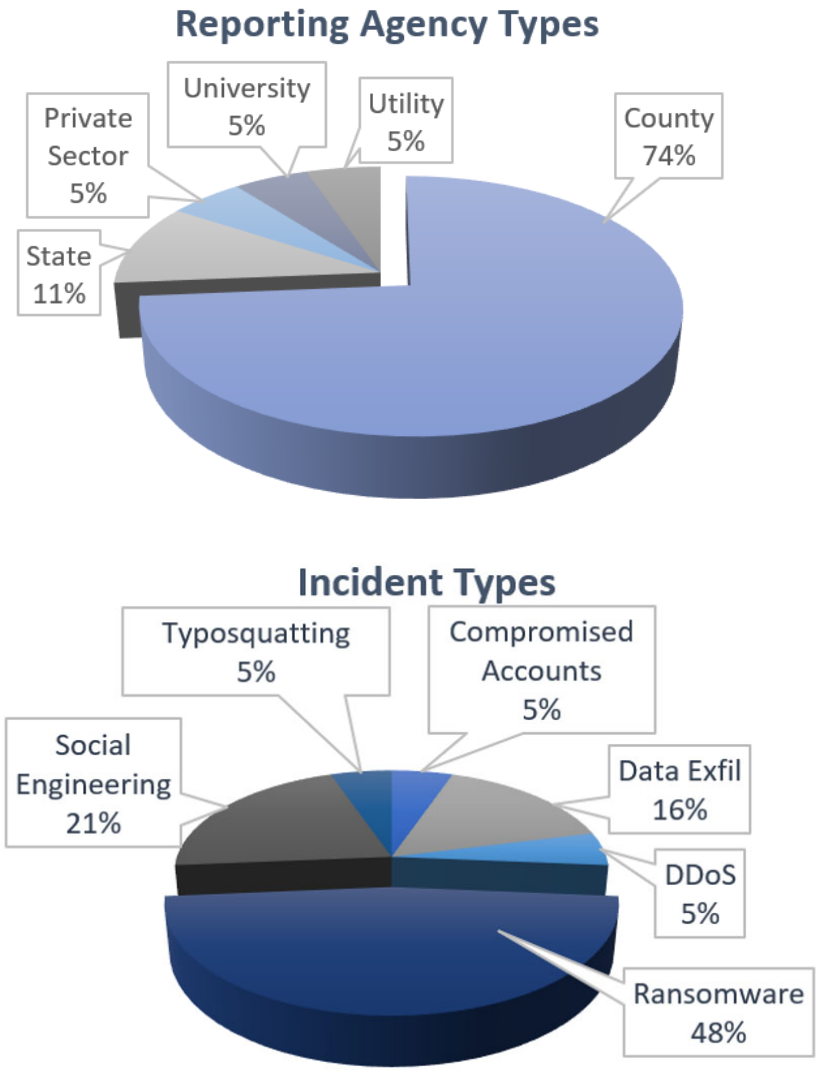


Figure 2: Data collected from the state cyber reporting data showing agency & incident type

(U) *What is a Data Breach?*

A data breach is an incident where information is stolen or taken from a system without the knowledge or authorization of the system's owner. IBM released a list of the initial attack vectors allowing a data breach to occur on a network. The top 4 attack vectors (based off occurrences) are as follows:

- Stolen or compromised credentials
- Phishing
- Cloud misconfigurations
- Vulnerabilities in third-party software

(U) *The Price of PII*

PII when sold on a dark web marketplace is usually advertised as having full credentials but are commonly referred to as "fullz". A single fullz will usually contain an individual's social security number, name, and birthday. The average price for a single US fullz is around $8; thus compromised data is routinely sold in bundles to make it profitable. If a driver's license number or bank statements can be attached the pricing per fullz will also increase.

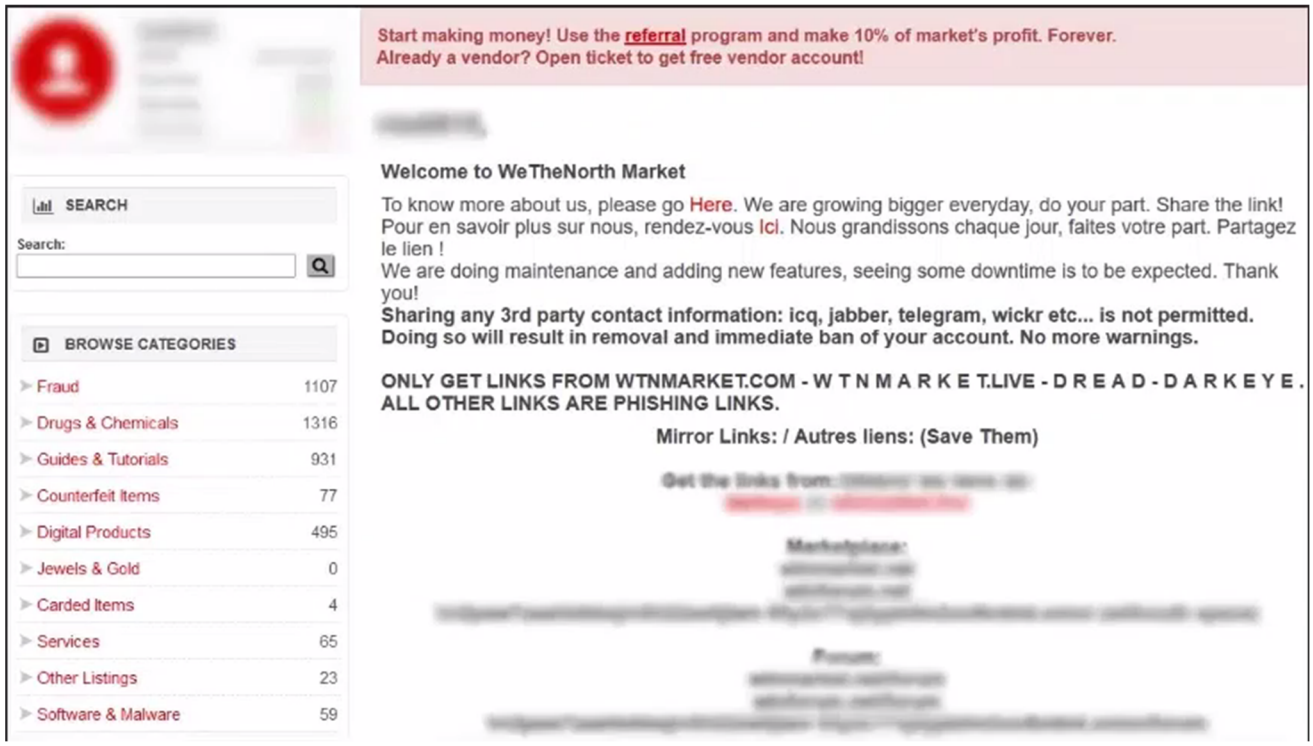


Figure 3: A screen capture of a dark web marketplace

(U) DOE's Stance on Protecting PII

The Chief Privacy and Information Security Officer for the Department of Education stated the following with regards to protecting student PII:

"There are several reasons why it is important to protect student personal identification information (PII).

First and foremost, protecting PII helps to prevent identity theft and other types of fraud. If a student's PII is compromised, it could be used to access their financial accounts, steal their identity, or commit other types of fraud using their name and other identifying information. This can have serious consequences for the student, including financial loss and damage to their reputation.

Second, protecting PII helps to maintain privacy and confidentiality. Students have a right to privacy and the protection of their personal information. When PII is not properly protected, it can be accessed and used without the student's knowledge or consent, which can be a violation of their privacy.

Finally, protecting PII is important for the security of educational institutions and their systems. If a student's PII is compromised, it could be used to gain unauthorized access to a school's systems or to carry out other types of cyberattacks. This can have serious consequences for the school, including financial loss, damage to its reputation, and disruption to its operations.

Protecting student PII is important to ensure the safety, privacy, and security of both individual students and educational institutions."

(U) Mitigating the Threat to Students

Parents may consider freezing their child's credit with the three major credit bureaus (Equifax, Experian, and TransUnion) so that it is less exploitable by cyber criminals. Once children are old enough to monitor and utilize their credit, their accounts can be unfrozen.

Children are highly susceptible to online schemes that target their personal information and possible security question answers. 'Social Quizzes' have been trending online and are popular "games" for children to play with their friends. These quizzes involve answering questions such as "what's your favorite color," or "what's your first pets name," and even "what was your first job/car". Answering questions such as the afore-mentioned quiz prompts lead to many people, not just students, revealing the answers they provide for password recovery which can allow threat actors access to their accounts. Although fun, these quizzes provide a lucrative opportunity for threat actors to obtain PII on students that will not change over time and may remain on internet servers for an indefinite period of time.

Aside from speaking with students about the importance of maintaining their online security and freezing their credit here are a few additional steps you can take to keep their PII secured.

- Implement Multifactor Authentication (MFA) on accounts created especially for banking.
- Monitor a child's health insurance claim information, it can indicate PII was used to access their benefits.
- Secure or shred physical documents with PII present on them. Threat actors can access a dumpster easier than an unsecured network.

Source, Reference, and Dissemination Information

Source Summary Statement	N/A
Definition	*((PM)* **FOUO:** For Official Use Only
Reporting Suspicious Activity	*(U)* **To report suspicious activity, law enforcement, Fire-EMS, private security personnel, and emergency managers should follow established protocols; all other personnel should call 911 or contact local law enforcement.** Suspicious activity reports (SARs) will be forwarded to the appropriate fusion center and FBI Joint Terrorism Task Force for further action. For more information on the Nationwide SAR Initiative, visit http://nsi.ncirc.gov/resources.aspx. *(U)* **To report a cyber security incident, submissions should be made to the GEMA/HS Cyber-Security Incident Portal.** An incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. In general, types of activity commonly recognized as violating typical security policies include attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally identifiable information; unwanted disruption or denial of service; the unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software without the owner's knowledge, instruction, or consent.
Dissemination	*(U//FOUO)* Federal, State, and Local officials, homeland security advisors, fusion center directors, emergency management directors, and school officials.
Warning Notices & Handling Caveats	*(U//FOUO)* This GEMA/HS Intelligence Unit document contains information that is FOR OFFICIAL USE ONLY. This product is comprised of open source and internal reporting (subject to change) with the intent to inform the public safety and emergency management community about issues named within. Further distribution without GEMA/HS Intelligence Unit authorization is strictly prohibited. Precautions should be taken to ensure this information is stored and/or destroyed in a manner that precludes unauthorized access. Dissemination to the media or public is not authorized.