CIRMA

School Announcement

Remote Learning Technology Liability

Background

The FBI has seen a rise in attempts by cyber predators to target children since the start of the pandemic. According to the FBI's Crimes Against Children and Human Trafficking Task Force, "These individuals are well aware that kids are spending more time on their devices and computers right now and see it as a target-rich environment to exploit." As schools continue to distribute technology to allow students to learn remotely, staff must also develop and implement plans to monitor student activity on school-owned equipment.

Scenario

The incident involved a female middle school student (Victim) attending the Collingswood Public School District (NJ). Victim (12-years old) was provided and used a school-issued laptop to assist with completing class assignments, homework and other projects. The school-issued computer did not have proper limitations or controls installed by the school which should have prevented the victim from accessing unauthorized or inappropriate sites or from preventing outside third parties from contacting the victim.

The 23-year old assailant, a Florida resident, contacted the victim through a search engine known as "Discord," where he had created an anime page for fans some time during the 2017-18 school year. The assailant and the victim communicated with each other every day. The assailant regularly urged the victim to provide him with "sexually provocative images of herself" and repeatedly expressed a desire to enter into a sexual relationship. After frequent online chats, the assailant told the victim he was traveling to New Jersey and wanted to meet with her and that if she would not meet with him, he would hurt himself.

After manipulating and coercing the victim, the assailant met the victim on March 29, 2019 in a local park. At this time, the assailant kidnapped the victim and took her on public transportation to a hotel in Philadelphia, where he sexually assaulted her over the course of 36 hours. After not returning home for the evening, the victim's parents contacted local law enforcement and reported her missing.

After an extensive search and with the cooperation of several public and private partners, law enforcement was able to "track" the victim's cell phone to the hotel where the victim was being assaulted. Law enforcement responded to the hotel, rescued the victim and transported her to a local hospital where she was cared for and reunited with her parents. The assailant was arrested and charged. Assailant later pleaded guilty to all charges and sentenced to 15 years in prison. As part of the sentencing order, the assailant will be required to be supervised by the court system and law enforcement for life, according to the documents released.

Damages

The parents of the victim brought forward a lawsuit against the school district alleging:

- The district failed to limit or monitor students' usage of school-issued computers.
- The school-issued computer did not have the "proper limitations or control" installed to prevent students from accessing unauthorized or inappropriate websites and that it failed to prevent third parties from contacting students.
- The district failed to have safety policies that address e-mail and chatrooms and failed to adopt county, state or federal internet safety protocols.
- That a guidance counselor at the school was aware of the student's contact with the assailant and never notified the parents or called the police.
- That school district officials ignored their requests to see their daughter's online browser history before she was kidnapped, attacked, or assaulted.

On the advice of the district's legal counsel, the school district entered into a settlement with the victim and her parents resolving all allegations against the school district, the school board and the guidance counselor for $950,000, in addition to compensating the victim and her family for legal fees. The district agreed to pay the settlement in the following manner:

- $650,000 in structured payments to the victim
- $300,000 to her parents for emotional distress

- Continued next page

CIRMA

School Announcement

LESSONS LEARNED

Implement a District Internet Security Policy. Set all school-owned technology to block inappropriate sites, unauthorized chat rooms, and unauthorized social media platforms. Limit the ability for third parties to communicate with students on district-owned devices.

Implement a District Internet Monitoring Protocol. Establish the ability to monitor sites visited by students when using school-issued devices remotely. This may include notifying teachers, administration or IT personnel when inappropriate content, sites or platforms are visited by those using the device.

Update Device Security Settings. Ensure that school-owned devices' privacy settings are set to the strictest level possible for online usage. Students should not have administrator access and should not be able to change security settings.

Develop a Technology Use Agreement. Require parents and guardians to sign and return the agreement prior to the device being issued to the student. The agreement should inform and educate them on the device settings, security, and expected use behaviors of the user (students). Parents and guardians should be expected to sign the technology use agreement understanding the protections that the school district has in place, their expected roles, and consequences for not enforcing the expected use policy.

Enforce Mandated Reporting Laws. Ensure that all staff are properly trained, as required by state law, on their role as a mandated reporter, reporting requirements, and the district's internal reporting protocols. Implement consequences and discipline in accordance with current collective bargaining agreements of those identified as mandated reporters who do not follow state law and/or district policy.

For more information on this topic, please contact your CIRMA Risk Management Consultant. Visit our training schedule at CIRMA.org for a list of current training programs.

Connecticut Interlocal Risk Management Agency