

Cyberbullying & Cyber Threats to Young People



By Lexie Williams

Resource Type: Articles

Topic: Data Privacy, Tech Risk, Cybersecurity, Youth Protection and Child Safety

In August of 2009, a nonprofit college preparatory day school in Los Angeles was sued for \$100 million dollars by a student's parents following a case of on-site cyberbullying. The incident occurred when nine students accessed another student's personal website from school computers and left death threats. The lawsuit alleged negligence committed by the school, as well as assault with death threats and hate crimes, invasion of privacy, and conspiracy. The victim's parents blamed the school for failing to protect their son, and for failing to punish the bullies. This type of cyberbullying case—stemming entirely from actions that take place online—is not uncommon, and with society's increasing reliance on technology, cyberbullying incidents are becoming more prevalent. Cyberbullying not only poses a risk for schools, but also for any youth-serving organization and certainly for the vulnerable children and teens served by these agencies.

Cyberbullying and the “Real World”

For many individuals, a disconnect exists between cyberbullying and traditional bullying, or harm that occurs in the physical world. Nonprofit leaders may wonder, “how could online bullying and cyber threats really affect my nonprofit, if the events only take place online?” Alas, liability can arise no matter where a violation occurs—in the physical world or the digital dimension. Even when cyberbullying or cyber threats transpire away from your nonprofit's facilities or program sites, they can significantly impact relationships within your organization, and potentially lead to lawsuits and other consequences if you fail to take the appropriate steps to prevent or stop the bullying. In the Los Angeles prep school case, the bullying students could have chosen to progress to bullying the victim in person on the school premises. In turn, the victim could have been physically harmed, and the bullying may have affected students other than the initial victim (e.g., witnesses, additional victims, etc.). In response to being physically or publicly bullied, the victim may have chosen to act out against his bullies, and potentially cause them harm in return. In this type of situation, the school would face countless consequences such as reconciling with devastated or enraged parents, providing care to frightened youth and compassion to the victim's family, and enduring hawk-like public scrutiny and negative press, not to mention lawsuits and other financial consequences. Any number of underlying conditions could create an environment in which cyberbullying is more likely to occur or to transform into physical bullying. Fortunately, in this case, cyberbullying was the sole offense, and the victim responded appropriately by immediately notifying his parents. Imagine this type of situation occurring at your organization—how would you respond? Armed with an understanding of the cyberbullying and cyber threat landscape, you can prepare to protect your young service recipients in the digital dimension: a place where today's youth spend considerable time, often alone or unsupervised, and with

little caution or regard for their own privacy and safety.

Cyberbullying versus Cyber Threats

Due to our constant use of technology and the growing risk of liability stemming from cyber crimes, you have likely heard the terms *cyberbullying* and *cyber threats*, but you may not be able to distinguish between the two. According to the i-SAFE Foundation (isafe.org), an organization dedicated to protecting the privacy of youth (partly by educating them to safely and responsibly use information and communications technology), **more than one in three young people have encountered cyber threats online**— A *cyber threat* is defined as any form of intimidating online material suggesting that the author or perpetrator may commit an act of violence, suicide, or self-harm. The Cyberbullying Research Center (cyberbullying.org) attests that more than half of youth and teens have been cyberbullying victims, and around 10% to 20% experience cyberbullying regularly. Phones are a popular cyberbullying channel due to their popularity and high-usage rate amongst teens, and it is estimated that fewer than 20% of young cyberbullying victims notify their parents that they have been bullied.

Understanding Cyberbullying

The U.S. Department of Health and Human Services maintains stopbullying.gov, which is designed to provide education and resources to prevent bullying behaviors. On the site, *cyberbullying* is defined as bullying that takes place using electronic technology such as social media websites, text messages, chat tools or other types of websites. Common cyberbullying tactics include:

- **Flaming**—writing content intended to evoke responses of fear, rage, humiliation, or other negative emotions.
- **Harassment**—creating and sending offensive, vulgar, or insulting messages on a continuing basis.
- **Denigration**—spreading or posting information about a person intended to damage his or her reputation.
- **Impersonation**—posing as someone other than yourself or using someone else's identity to break into an account that does not belong to you, with the intent to cause harm to another's reputation or well-being.
- **Outing and Trickery**—coercing someone to share private information or images with you and then sharing this information online or via text message without consent for the purpose of embarrassing the individual.
- **Exclusion**—directly or indirectly sending a hurtful message to a target victim implying that they are not being included in social activities, or are disliked or should be ostracized by others.
- **Cyberstalking**—repeatedly sending intimidating messages to a target victim or threatening to harm the safety of the victim or someone to whom they are close.

Risk Factors

According to the U.S. Department of Health and Human Services, there are several risk factors that can help responsible adults identify youth who may be more susceptible to becoming bullies or to being bullied than other children. Young people who have difficulty interacting or connecting with others in-person are often the most likely to engage in risky online behavior; thus, children who display some of the following attributes may be more likely to bully others:

- Easily frustrated or impulsively angry/violent
- Obsessed or very interested in discussing violence or violent behaviors
- Difficulties at home, or low parental involvement in their lives
- Frequently berate peers and other youth
- Have difficulty following guidelines and rules for acceptable behavior
- Question authority or act defiantly toward adults or other authority figures

Children who are the victims of bullying often possess one or more of the following risk factors:

- Seen as somehow different from their peers (e.g., 'nerdy,' immature, irritating, attention-seeking, etc.)
- Prone to low self-confidence or mental health challenges such as depression or anxiety

- Perceived as weak or incapable of standing up for themselves
- Tend to isolate themselves from others
- Have mental, physical, or learning disabilities
- Identify as lesbian, gay, bisexual, or transgender (LGBT)

Enhancing Your Organization's Preventive Measures Against Cyberbullying

According to the Juvenile Justice Information Exchange (jjie.org), establishing a 'zero tolerance' policy for bullying is not enough to combat this pervasive issue. These types of policies have been linked to higher school dropout rates and increased incarceration rates, sometimes with little effect on the issue they actually mean to address. Advocates from the Teaching Tolerance Project (tolerance.org), recommend using one of two techniques to manifest a culture of acceptance and to limit cyberbullying: *reparative justice* or *behavior contracts*.

Reparative justice approaches rule violation by aiming to repair the relationships between all individuals impacted by the misbehavior (including the perpetrator) instead of assigning blame. This mediation method requires organizations to make careful selections of adults who are assigned to intervene. These caretakers must have good listening and communication skills, impartiality, and patience. While time-consuming, this unconventional technique allows all parties involved to move forward in a mutual fashion. If effective, this technique could aid not only a cyberbullying victim, but it could also aid the bully and reduce the likelihood that the bully will act out again.

Nonprofits looking for a quick preventative measure should consider writing behavior contracts to distribute to youth and teens who are served by the organization. The contract should define your organization's policy on technology use, explain how misconduct will be handled, and require each participant to sign in agreement to the policy, prior to being allowed to use the Internet or technology during their time at your nonprofit. To make behavior contracts more effective, continue offering training and supervision (as appropriate), to youth who are using your technology resources. For example, youth may find it easier to understand and follow your protocols if they are offered refresher training on the technology use policy, or other guidance on safe uses of the Internet. Using behavior contracts or implementing reparative justice techniques will help bring your nonprofit one step closer to a culture of acceptance, inclusion, and proactive youth protection.

Fortunately, your organization can take even more preventative measures to avoid becoming the next big 'cyber no-no' headline. Some of these measures include:

- Establishing consequences for youth who misuse technology (e.g. loss of technology use privileges), and creating a process by which parents are informed in these situations.
- Reassuring the youth within your organization that being bullied is never their fault, and providing training on what to do when you are the victim of bullying, or what to do when you see another youth being bullied (e.g., reporting, bystander intervention training, etc.).
- Informing new youth participants of your nonprofit's rules on the use of technology and your commitment to ensuring that all individuals are treated respectfully at all times, including online.
- Keeping computers and other technology in a shared area where staff and volunteers are able to monitor computer use.
- Organizing a viewing of cyberbullying movies such as *Cyberbully* and *Submit the Documentary: The Virtual Reality of Cyberbullying*.

To start creating a cyberbullying policy and training program for your young participants, try out the following ideas:

- Emphasize the effects of cyberbullying on not only victims, but also the perpetrators.
- Encourage youth and teens to save or take pictures of cyberbullying (or other types of bullying) as proof that it occurred, in case the organization, parents, or authorities need to get involved.
- Inform youth and teens that they should never reveal social media or Internet passwords to anyone aside from a parent or trusted adult. Written copies of passwords should be stored in an area where they are unlikely to be found by unauthorized individuals.
- Reiterate to youth and teens that they should not share anything through text or the Internet that they

would not want to be made publicly known. Remind youth that the people they communicate with via technology may not be who they say they are, and that electronic messages are not always secure.

- Convey the importance of protecting personal information online, and explain the risks related to meeting an online acquaintance in person.

For more information about cyber risks and creating an effective program to protect your young participants from harm, see the Centers for Disease Control and Prevention (CDC) tip sheet

(www.cdc.gov/violenceprevention/pdf/ea-tipsheet-a.pdf) on protecting children from online aggression, or visit the U.S. Department of Health and Human Services' stopbullying.gov website to find statistics on bullying, and to learn about implementing bullying education and prevention techniques at your nonprofit.

Lexie Williams was a 2015 Summer Risk Management Intern at the Nonprofit Risk Management Center.

Questions about the topics covered in this article can be directed to info@nonprofitrisk.org or 703.777.3504.