School Safety Newsletter

Volume 2, Issue 3 October 2014

Local Law Enforcement Launch New Campaign to Curb Social Media During Emergencies

By Josh Kerns on July 30, 2014

Moments after a gunman opened fire on the Seattle Pacific University campus in June, social media exploded as people took to Twitter and other networks to report what was going on.

A number of students tweeted where they were sheltering, while other people posted pictures of the scene unfolding as police swarmed in.

Although a heroic student was able to quickly incapacitate the gunman after he shot several people, Officials worry all of the postings could have ultimately led to a much greater tragedy.

"Sooner or later we'll have an emergency where the suspect is watching social media. That could allow an offender to escape, or possibly even cost an officer their life," says Washington State Patrol Chief John R. Batiste.

After other recent shootings in Moncton, New Brunswick and Portland, OR, a number of Puget Sound area agencies decided they needed to do something to get the word out about the potential dangers of sharing too much during an emergency, launching a new campaign this week called "Tweet Smart."

"We had seen agencies try to do that in the middle of an emergency. They've got the active shooter running around and they're seeing people posting stuff and they're saying 'please don't do that'...and the cat's already out of the bag," says WSP spokesman Bob Calkins. "So our goal was to get out ahead of that and make it a part of social media culture."

It's a growing problem that first came to light for local law enforcement following the November 2009 shooting of four Lakewood police officers. As Seattle police surrounded a park in search of suspect Maurice Clemons, a number of people reported police movements on Twitter.

"If he was there or paying attention and watching a hashtag, that is absolutely the kind of thing that could become a problem," Calkins says.

Mainstream media have worked with law enforcement for years to limit the reporting of sensitive information during critical times. But with the prevalence of smartphones and social media, there can be hundreds of people posting information and photos in real time.

"When we're on big scenes that draw a crowd, almost immediately you see the arms go up with the cameras, which is fine. It's what you do after that's the problem," says Asst. Chief Mike Zaro with the Lakewood Police Department.

"I don't think they're doing it maliciously. I just think they haven't been made aware of what some of the risks of that are," he says.

The "Tweet Smart" campaign is a partnership with a number of law enforcement agencies including the WSP, Bellevue, Des Moines, Federal Way, King County, Kitsap County, Lakewood and Seattle.

Officials say they're not trying to deter people from posting pictures altogether, but to avoid posting officers' movement and other tactical information that could put lives at risk.

Protecting our future through information sharing

In This Issue

Local Law Enforcement Launch New Campaign to Curb Social Media During Emergencies (continued)

"If it's safe to do so, go ahead and take pictures of our deputies in action," says Kitsap County Sheriff Steve Boyer. "We're very proud of the work they do. We'd simply ask that you wait to post those pictures until the emergency is over."

The campaign includes a list of suggested do's and don'ts law enforcement hopes people will keep in mind during an emergency:

-Do get to a safe place and call 911 if possible. Live telephone calls to dispatchers are law enforcement's best source of real-time information in an emergency.

-Do feel free to let family and friends know you've reached safety.

-Do feel free to warn friends if you have first-hand knowledge of a developing emergency.

-Don't tweet or post about the movements of police, or post pictures of officers. Even what seems like vague information could be used by a criminal familiar with the area.

-Don't endanger yourself to get a picture, no matter how compelling.

-Don't spread rumors. If you're not sure, don't post, tweet or re-tweet.

-Do feel free to tweet about the response and post pictures after the emergency is over.

Calkins acknowledges the campaign won't completely stem the tide of social media during an emergency, but he says law enforcement hopes it can start a conversation that will make people think twice before posting in the middle of an unfolding incident.

"The "Twittershpere" has a very strong culture. We're hoping to make this safety item a part of their culture," he says.

http://mynorthwest.com/11/2576474/Local-law-enforcement-launch-new-campaign-to-curb-social-media-during-emergencies

You can find another recent article on the same topic titled, "Using Social Media in Times of Crisis—Harmful or Helpful? Twitter and Facebook can provide immediate alerts and responses, but also yield misinformation and other potential concerns." by Ralph Metzner, August 11, 2014 at http://www.campussafetymagazine.com/article/using_social_media_in_times_of_crisis_harmful_or_helpful/P2

Just in Time Research: Data Breaches in Higher Education

Full 2014 article can be found: https://net.educause.edu/ir/library/pdf/ecp1402.pdf

Hardly a day goes by without a media report about a data breach that exposes the personally identifiable information (PII) of individuals. While much of the news regarding data breaches focuses on the harm to affected individuals, data breaches also harm the organization experiencing the breach. Potential direct financial costs of a data breach include legal representation, fines (depending on the nature of the breach), and the expense of notifying affected individuals. Organizations also face losses in reputation and consumer confidence. Particularly important for higher education institutions are reputational consequences, which could result in a loss of alumni donations and even a reduction in the number of students choosing to apply to or attend the institution.

Since 2005, the Privacy Rights Clearinghouse (PRC) has worked to document how technology affects individual privacy and to educate consumers on how to protect their privacy.1 The PRC also collects information on verifiable data breaches in the United States and the number of records containing PII exposed in those breaches. As of April 25, 2014, the PRC Chronology of Data Breaches had documented 4,257 data breaches in the United States involving at least 867,217,832 records from all industry sectors, including but not limited to education.

Monthly Webinars!

First Wednesday of Every Month at 10 am.

Next Webinar - Oct 29, 2014

Each webinar has a round table discussion at the end. Questions are always welcome!

To participate, you must be a vetted member. For more information please email schoolsafety@isp.state.il.us

Just in Time Research: Data Breaches in Higher Education (continued)

The PRC database includes 727 breaches involving educational institutions that were made public in 2005–2014, involving more than 14 million breached records. The number of breaches includes breaches attributed to higher education institutions as well as trade schools, K–12 schools and school districts, and education-related nonprofit organizations.

The PRC notes that the number of records exposed in the reported data breaches may actually be larger than the numbers they capture in their database. This is because the number of records exposed in many data breaches cannot be known. Upon review of the PRC dataset, 73% of breaches attributed to the education sector included data about the number of records exposed per breach. While that leaves over a quarter of education's breaches with an unknown number of records, that is lower than for any other sector in the PRC data. Due to this missing information, the total number of records affected by all breaches in the PRC database is likely two to three times larger than the currently reported total. This report focuses predominantly on the number of breach incidents reported, rather than the number of records exposed in those breaches, due to the large number of breaches with unknown records.

The Number of Reported Breaches Varies By Carnegie Class

Seventy-seven percent of the breaches attributed to educational institutions in the PRC Chronology of Data Breaches occurred at colleges and universities. From 2005 to 2013, there were 551 breach reports made by colleges and universities—a rate of just over one per week. While the data hint at a downward trend in the number of breaches reported over time, it is too early to tell whether this is a significant trend (figure 2).

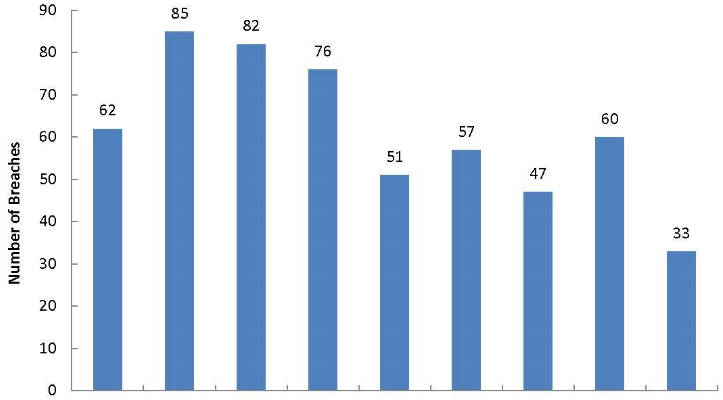

Figure 2. Number of higher education reported breaches per year, 2005–2013 (ECAR data set, n = 551)

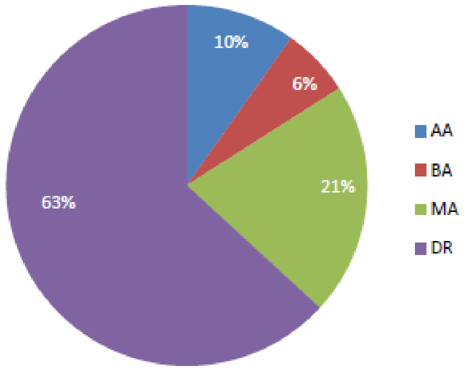

Figure 3. Breaches by Carnegie Classification, 2005–2013 (ECAR data set, n = 551)

Doctoral (DR) institutions are responsible for the majority of reported breaches, which is likely a function of scale (e.g., larger campuses, distributed environments, more complicated information systems, more records to manage, etc.; figure 3). Sixty-three percent of the PRC reported breaches are attributed to DR institutions, though they make up only 7% of all U.S. institutions. Twenty-one percent of the reported breaches are attributed to master's (MA) institutions, which make up 16% of all U.S. institutions. While they comprise the majority of U.S. higher education institutions, associate's (AA) and bachelor's (BA) institutions had fewer reported data breaches.

DR and MA institutions are most likely to have experienced more than one breach reported in the PRC. Fifty-four percent of DR institutions with breaches—or one-quarter of all the DR institutions in the United States—have had more than one reported breach. Twenty-one MA institutions had more than one reported breach in the PRC. AA and BA institutions were significantly less likely to have more than one reported breach (figure 5—next page).

Unintended Disclosures and Hacking/Malware Are the Most Common Breaches in Higher Education

The PRC Chronology of Data Breaches classifies breaches into eight categories:

- **Payment Card Fraud (CARD):** Fraud involving debit and credit cards that is not accomplished via hacking.
- **Unintended disclosure (DISC):** Sensitive information posted publicly on a website, mishandled, or sent to the wrong party via e-mail, fax, or mail.

New Study Examines Likelihood of Students Reporting a Weapon on Campus

September 19, 2014

http://www.campussafetymagazine.com/article/new_study_examines_likelihood_of_students_reporting_a_weapon_on_campus?utm_source=newsletter&utm_medium=email&utm_campaign=enewstuesday

A University of Texas Dallas study shows certain factors affect a student's willingness to report having seen a weapon at school. The study was published online in "Youth Violence and Juvenile Justice" and it used data from anonymous online surveys administered to students in grades 9-12 at 10 schools in a northeastern U.S. state between 2008 and 2011.

According to the study, 76 percent of students who responded to the survey said they would report having seen a knife on campus. Eighty six percent said they would report a gun on campus. For both male and female students, high academic achievement was associated with an increased willingness to report a gun or a knife. A stronger school attachment resulted in an increased willingness to report a knife.

For both genders, having previously seen a weapon on campus decreased a student's likelihood of reporting a knife. For male students, even prior knowledge of a weapon on campus reduced willingness to report a knife. Approximately 34 percent of survey respondents reported having seen or having prior knowledge of a weapon on campus in the last three months.

Another major factor in the intent to report a weapon on campus was knowledge of at least two school security measures such as ID badges, locker checks, visitor sign-in sheets, etc. Although most students said they would report seeing a weapon on campus, they were least likely to reveal that information to a principal or counselor. They were most likely to report it to their parents or to a family member. Only a small subgroup of students said they would not report a weapon on campus to anyone.

Just in Time Research: Data Breaches in Higher Education

- **Hacking or malware (HACK):** Electronic entry by an outside party; data loss via malware and spyware.
- **Insider (INSD):** Intentional breach of information by someone with legitimate access (e.g., an employee or contractor).
- **Physical loss (PHYS):** Lost, discarded, or stolen nonelectronic records, such as paper documents.
- **Portable device (PORT):** Lost, discarded, or stolen portable devices (e.g., laptop, PDA, smartphone, portable memory device, CD, hard drive, data tape, etc.).
- **Stationary device (STAT):** Lost, discarded, or stolen stationary electronic device such as a computer or server not designed for mobility.
- **Unknown or other (UNKN):** Breaches that do not fit into the above categories or where a root cause has not been determined.

In higher education, the largest proportion of the reported breaches fall into the hacking/malware classification (36%). These are breaches where an outside party accessed records via direct entry, malware, or spyware. Thirty percent of the reported breaches were the result of unintended disclosure, where sensitive information was inadvertently made publicly available on a website or sent to an unintended recipient via e-mail or fax. Seventeen percent of the reported breaches were due to the loss of a portable device, such as a lost or stolen laptop or memory device (figure 6). Payment card fraud (CARD) is the least likely data breach classification seen among the reported breaches at higher education institutions. Only one breach, which occurred in 2012, was classified with this tag.

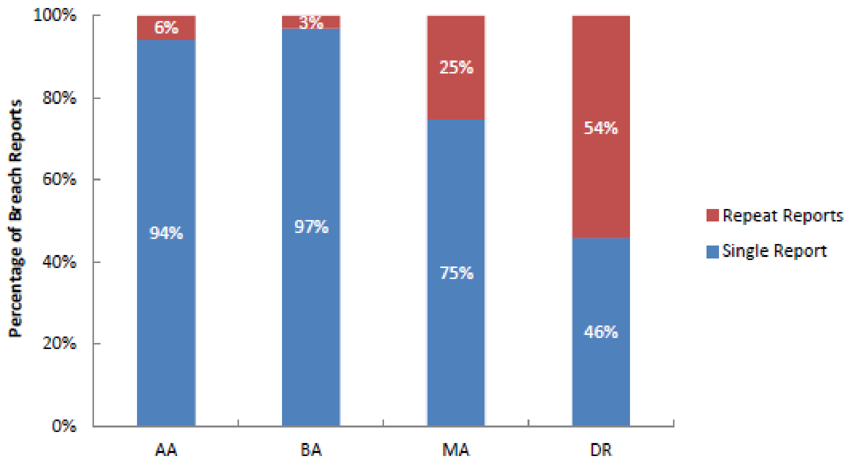

Figure 5. Proportion of single/repeat breach reports by Carnegie Classification in the PRC, 2005–2014 (ECAR data set, n = 324)

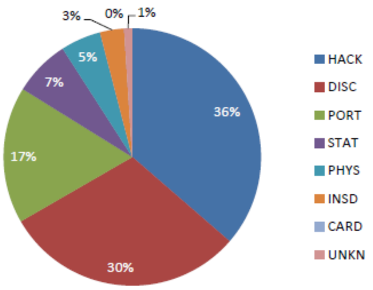

Figure 6. Types of data breaches in higher education, 2005–2013 (ECAR data set, n = 551)

Mia Langheim

School Intelligence Officer

School Safety Newsletter

Statewide Terrorism & Intelligence Center
2200 S. Dirksen Parkway
Springfield, IL 62703
Phone: 217-558-2661
E-Mail: schoolsafety@isp.state.il.us