

Study: Teens more likely to smoke pot than cigarettes

By Marisa Taylor, Aljazeera America

High school students are more likely to smoke marijuana on a daily basis than they are to smoke cigarettes, according to an annual government survey of drug, alcohol and tobacco use released Wednesday.

About 6 percent of 12th grade students reported that they smoked pot on a daily basis, about the same proportion as in 2014. But just 5.5 percent of high school seniors reported smoking tobacco cigarettes every day, down from 6.7 percent in 2014. It marks the first time since the survey was first conducted in 1975 that daily marijuana use has eclipsed smoking.

The perception of marijuana as “risky” has declined steadily, with 31.9 percent of seniors saying that regular marijuana use may be harmful, down from 36.1 percent in 2014.

[Read the whole story](#)

Opinion: LV Fire defends ambulance staffing

By Kileigh Labrado

It has been and will remain the mission of the Lake Valley Fire Protection District to provide the highest level of public safety services for our community, its people, and

the environment. As our motto states, it is "Because We Care".

Driven by these guiding principles, in 2001 the LVFPD entered into a partnership with the city of South Lake Tahoe to provide fire based ambulance transportation and advanced life support paramedic services throughout the South Shore of Lake Tahoe. For over 14 years the fire district has had the privilege to provide first class fire based emergency medical services (EMS) to our constituents under contracts with the county of El Dorado. LVFPD remains dedicated to providing the highest level of public safety to the community we proudly serve.

The partnership between the Lake Valley Fire Protection District and the city of South Lake Tahoe formed the Cal-Tahoe JPA which currently has a contract with the county of El Dorado to provide paramedic ambulance services to the South Shore until Aug. 31, 2019, with the potential to extend the contract until Aug. 31, 2021. The JPA partnership allowed ambulances to be staffed with firefighter/paramedics in the South Shore, which increased the level of public safety by increasing the number of firefighters on duty every day. Firefighter/paramedics are available for all types of incidents including fires, rescues, and vehicle accidents as well as medical aids.

On Dec. 14, 2015, the city of South Lake Tahoe began staffing the two JPA ambulances they are responsible for staffing with non-firefighters. While non-firefighting paramedics and emergency medical technicians are qualified to run medical aid calls, they are not all risk personnel and cannot perform the same duties of a firefighter, such as fighting fires, entering burning buildings, performing technical rescues, or vehicle extrication.

There have been ongoing discussion and negotiations between the city and LVFPD regarding LVFPD taking over staffing of all of the ambulances in the South Shore to keep a fire based

system intact. Unfortunately there has been no agreement reached to date. The LVFPD is committed to working with the city and the county to find an equitable solution that is in the best interest of the community and maintains the increased level of public safety.

Lake Valley Fire Protection District strongly believes that a fire based emergency medical and ambulance transport service for the South Shore provides our constituents with a proper level of public safety. The fire district believes that the ambulance transport services agreement enhances our ability to maintain an adequate work force that is needed to adequately fulfill our mission and commitment to provide a high level of public safety to the community we proudly serve. Public safety and fiscal responsibility are of the utmost importance to the fire district. It is the intention of the LVFPD to continue to operate fire based emergency medical and ambulance transport services for our constituents.

Kileigh Labrado is the public information officer for Lake Valley Fire Protection District.

Consumers buying cheaper Christmas gifts

By Joyce M. Rosenberg, AP

Cheap is the new chic for holiday gifts.

Jana Montero, who has in the past bought loved ones iPods and tablets for Christmas, has changed her attitude about gift giving: This holiday season, she's grabbing candle sets and serving dishes that cost under \$30 to give to family and

friends.

Montero, who lives in New York and is saving to buy a home with her husband, said: "We want to make sure we're conscious of what we're spending."

More holiday shoppers are expected to be like Montero this holiday season in the latest twist in a theme that has played out since the recession. For nearly a decade, shoppers have been more cautious and practical about their spending, doing more bargain shopping and hunting for deals. But recently, shoppers have taken that practice a step further.

They're becoming more open to buying gifts that in the past might have been considered downright cheap. So, they're not just looking for big discounts on extravagant, expensive designer and brand name goods; they're starting out with the intention of getting less expensive items that they might not have considered buying as gifts in the past.

The number of people willing to buy gifts during this holiday shopping season for under \$10 rose to 4 percent this year from 1 percent last year, according to a survey of 1,000 people by America's Research Group, a firm that researches consumer behavior. Meanwhile, the number of people willing to spend between \$26 and \$35 fell to 18 percent from 22 percent.

Overall, people are expected to spend modestly more this holiday season. The National Retail Federation predicts holiday spending in November and December will be up 3.7 percent to \$630.5 billion this year, slower than the 4.1 percent growth during the same period last year.

The shift in attitude toward cheap is partly rooted in economics, says Jeff Green, a retailing consultant based in Phoenix. Shoppers who vigilantly watched their budgets during the recession continue to feel the pressure of keeping tabs on what they're spending even as the economy improves. "Even with the unemployment rate down, I don't think people feel secure

in their jobs,” he says.

But it’s also rooted in a change in consumer psychology. Some shoppers have become suspicious of retailers who continually slash prices, retail consultant Paco Underhill says. In other words, people are beginning to question whether they’re paying too much for the gifts that they’re buying, so now they’re starting out with the expectation that they’ll buy really cheap items.

“One of the deeply confusing elements to the consuming public is: What is the real cost of something?” he says.

For example, Stacy Roberts saw plenty of sales when she visited The Fashion Mall at Keystone in Indianapolis on Saturday, but she wasn’t impressed. She said shoppers need to start following the price of something they want to buy for the holidays a few months beforehand, so they can tell if the sales are truly a bargain.

“To me, deals are B.S.,” she says.

Adding to the mistrust of “deals,” some consumer marketing experts say, is the shedding of the stigma associated with buying smaller, less expensive gifts. People who spend less can be perceived as savvy shoppers, and also warmer and friendlier than someone who’s a conspicuous consumer, says Maura Scott, a marketing professor at Florida State University.

The growing willingness of holiday shoppers to spend less on gifts has made storeowners more conservative as they’ve stocked up for the holidays. Many have more lower-priced merchandise on their shelves to cater to the growing prevalence of cheap-gift buyers.

Toys R Us has bins throughout its stores that feature merchandise like race cars and stuffed animals for less than \$10, and has a section called Dollar Shop with toys priced \$1

to \$5. Target stores have a section called Bullseye's Playground with \$5 and under items including toys and accessories for electronics.

Smaller retail shops also are stocking up on more inexpensive items.

Elizabeth Madsen's inventory includes gift items \$30 and under at her Poughkeepsie, New York, clothing shop. Madsen says customers want to buy at a boutique, but are cautious about what they spend. So her store has items like \$10 key chains and \$22 sachets. They're selling well, even bringing in people who don't usually shop in her store, Elizabeth Boutique.

"If you have price options for people from lower to higher, you're going to have a better chance of grabbing the customer's attention," Madsen says.

Janae Melvin's attitudes about spending on gifts have changed, in part because she and her husband are putting money aside for a home and a big family vacation next year. Melvin, who lives in Kansas City, Kansas, is looking for gifts that don't cost as much as ones she gave in the past – "not cheap junk, but items that have meaning or significance."

Some of her children's gifts will be toys – dolls and action figures – that cost under \$10. They're each getting a \$25 membership in Sluggerrr's Blue Crew, the Kansas City Royals' children's club, which includes a pullover, baseball cap and necklace when they join. For some of her family members, Melvin is buying \$15 or \$20 picture frames and inserting a family photo.

"It's just not necessary to spend so much," she says.

Anne D'Innocenzio in New York and Tom Murphy in Indianapolis contributed to this report.

U.S. not prepared for power grid cyberattack

By Garance Burke and Jonathan Fahey, AP

Security researcher Brian Wallace was on the trail of hackers who had snatched a California university's housing files when he stumbled into a larger nightmare: Cyberattackers had opened a pathway into the networks running the United States power grid.

Digital clues pointed to Iranian hackers. And Wallace found that they had already taken passwords, as well as engineering drawings of dozens of power plants, at least one with the title "Mission Critical." The drawings were so detailed that experts say skilled attackers could have used them, along with other tools and malicious code, to knock out electricity flowing to millions of homes.

Wallace was astonished. But this breach, the Associated Press has found, was not unique.

About a dozen times in the last decade, sophisticated foreign hackers have gained enough remote access to control the operations networks that keep the lights on, according to top experts who spoke only on condition of anonymity due to the sensitive nature of the subject matter.

The public almost never learns the details about these types of attacks – they're rarer but also more intricate and potentially dangerous than data theft. Information about the government's response to these hacks is often protected and sometimes classified; many are never even reported to the government.

These intrusions have not caused the kind of cascading blackouts that are feared by the intelligence community. But so many attackers have stowed away in the systems that run the U.S. electric grid that experts say they likely have the capability to strike at will.

And that's what worries Wallace and other cybersecurity experts most.

"If the geopolitical situation changes and Iran wants to target these facilities, if they have this kind of information it will make it a lot easier," said Robert M. Lee, a former U.S. Air Force cyberwarfare operations officer. "It will also help them stay quiet and stealthy inside."

In 2012 and 2013, in well-publicized attacks, Russian hackers successfully sent and received encrypted commands to U.S. public utilities and power generators; some private firms concluded this was an effort to position interlopers to act in the event of a political crisis. And the Department of Homeland Security announced about a year ago that a separate hacking campaign, believed by some private firms to have Russian origins, had injected software with malware that allowed the attackers to spy on U.S. energy companies.

"You want to be stealth," said Lillian Ablon, a cybersecurity expert at the RAND Corporation. "That's the ultimate power, because when you need to do something you are already in place."

The hackers have gained access to an aging, outdated power system. Many of the substations and equipment that move power across the U.S. are decrepit and were never built with network security in mind; hooking the plants up to the Internet over the last decade has given hackers new backdoors in. Distant wind farms, home solar panels, smart meters and other networked devices must be remotely monitored and controlled, which opens up the broader system to fresh points of attack.

Hundreds of contractors sell software and equipment to energy companies, and attackers have successfully used those outside companies as a way to get inside networks tied to the grid.

Attributing attacks is notoriously tricky. Neither U.S. officials nor cybersecurity experts would or could say if the Islamic Republic of Iran was involved in the attack Wallace discovered involving Calpine Corp., a power producer with 82 plants operating in 18 states and Canada.

Private firms have alleged other recent hacks of networks and machinery tied to the U.S. power grid were carried out by teams from within Russia and China, some with governmental support.

Even the Islamic State group is trying to hack American power companies, a top Homeland Security official told industry executives in October.

Homeland Security spokesman SY Lee said that his agency is coordinating efforts to strengthen grid cybersecurity nationwide and to raise awareness about evolving threats to the electric sector through industry trainings and risk assessments. As Deputy Secretary Alejandro Mayorkas acknowledged in an interview, however, “we are not where we need to be” on cybersecurity.

That’s partly because the grid is largely privately owned and has entire sections that fall outside federal regulation, which experts argue leaves the industry poorly defended against a growing universe of hackers seeking to access its networks.

As Deputy Energy Secretary Elizabeth Sherwood Randall said in a speech earlier this year, “If we don’t protect the energy sector, we are putting every other sector of the economy in peril.”

The attack involving Calpine is particularly disturbing

because the cyberspies grabbed so much, according to interviews and previously unreported documents.

Cybersecurity experts say the breach began at least as far back as August 2013, and could still be going on today.

Calpine spokesman Brett Kerr said the company's information was stolen from a contractor that does business with Calpine. He said the stolen diagrams and passwords were old – some diagrams dated to 2002 – and presented no threat, though some outside experts disagree.

Kerr would not say whether the configuration of the power plants' operations networks – also valuable information – remained the same as when the intrusion occurred, or whether it was possible the attackers still had a foothold.

According to the AP investigation, the hackers got:

- User names and passwords that could be used to connect remotely to Calpine's networks, which were being maintained by a data security company. Even if some of the information was outdated, experts say skilled hackers could have found a way to update the passwords and slip past firewalls to get into the operations network. Eventually, they say, the intruders could shut down generating stations, foul communications networks and possibly cause a blackout near the plants.
- Detailed engineering drawings of networks and power stations from New York to California – 71 in all – showing the precise location of devices that communicate with gas turbines, boilers and other crucial equipment attackers would need to hack specific plants.
- Additional diagrams showing how those local plants transmit information back to the company's virtual cloud, knowledge attackers could use to mask their activity. For example, one map shows how information flows from the Agnews power plant in San Jose near the

San Francisco 49ers football stadium, to the company headquarters in Houston.

Wallace first came across the breach while tracking a new strain of noxious software that had been used to steal student housing files at the UC Santa Barbara.

“I saw a mention in our logs that the attackers stored their malware in some FTP servers online,” said Wallace, who had recently joined the Irvine-based cybersecurity firm Cylance Inc., fresh out of college. “It wasn’t even my job to look into it, but I just thought there had to be something more there.”

Wallace started digging. Soon, he found the FTP servers, typically used to transfer large numbers of files back and forth across the Internet, and the hackers’ ill-gotten data – a tranche of more than 19,000 stolen files from thousands of computers across the world, including key documents from Calpine.

Before Wallace could dive into the files, his first priority was to track where the hackers would strike next – and try to stop them.

He started staying up nights, often jittery on Red Bull, to reverse-engineer malware. He waited to get pinged that the intruders were at it again.

Months later, Wallace got the alert: From Internet Protocol addresses in Tehran, the hackers had deployed TinyZbot, a Trojan horse-style of software that the attackers used to gain backdoor access to their targets, log their keystrokes and take screen shots of their information. The hacking group, he would find, included members in the Netherlands, Canada, and the United Kingdom.

The more he followed their trail, the more nervous Wallace got. According to Cylance, the intruders had launched digital

offensives that netted information about Pakistan International Airlines, the Mexican oil giant Pemex, the Israel Institute of Technology and Navy Marine Corps Intranet, a legacy network of the U.S. military. None of the four responded to AP's request for comment.

Then he discovered evidence of the attackers' most terrifying heist – a folder containing dozens of engineers' diagrams of the Calpine power plants.

According to multiple sources, the drawings contained user names and passwords that an intruder would need to break through a firewall separating Calpine's communications and operations networks, then move around in the network where the turbines are controlled. The schematics also displayed the locations of devices inside the plants' process control networks that receive information from power-generating equipment. With those details, experts say skilled hackers could have penetrated the operations network and eventually shut down generating stations, possibly causing a blackout.

Cylance researchers said the intruders stored their stolen goods on seven unencrypted FTP servers requiring no authentication to access details about Calpine's plants. Jumbled in the folders was code that could be used to spread malware to other companies without being traced back to the attackers' computers, as well as handcrafted software designed to mask that the Internet Protocol addresses they were using were in Iran.

Circumstantial evidence such as snippets of Persian comments in the code helped investigators conclude that Iran was the source of the attacks.

Calpine didn't know its information had been compromised until it was informed by Cylance, Kerr said.

Iranian U.N. Mission spokesman Hamid Babaei did not return calls or address questions emailed by AP.

Cylance notified the FBI, which warned the U.S. energy sector in an unclassified bulletin last December that a group using Iran-based IP addresses had targeted the industry.

Whether there was any connection between the Iranian government and the individual hackers who Wallace traced – with the usernames parviz, Alireza, Kaj, Salman Ghazikhani and Bahman Mohebbi – is unclear.

Cyberattacks designed to steal information are steadily growing in scope and frequency; there have been high-profile hacks of Target, eBay and federal targets such as the U.S. Office of Personnel Management. But assaults on the power grid and other critical infrastructure aim to go a step further.

Trained, well-funded adversaries can gain control of physical assets – power plants, substations and transmission equipment. With extensive control, they could knock out the electricity vital to daily life and the economy, and endanger the flow of power to mass transportation, military installations and home refrigerators.

In summer 2014, a hacker of unknown origin, using masking software called Tor, took over the controls of a large utility's wind farm, according to a former industry compliance official who reviewed a report that was scrubbed of the utility's name. The hacker then changed an important setting, called the automatic voltage regulator, from "automatic" to "manual," he said.

That seemingly simple change to any power plant can damage the generator and destabilize parts of the nearby grid if the plant's output is high enough.

Last year, Homeland Security released several maps that showed a virtual hit list of critical infrastructure, including two substations in the San Francisco Bay area, water and gas

pipelines and a refinery. And according to a previously reported study by the Federal Energy Regulatory Commission, a coordinated attack on just nine critical power stations could cause a coast-to-coast blackout that could last months, far longer than the one that plunged the Northeast into darkness in 2003.

“The grid is a tough target, but a lucrative target,” said Keith Alexander, the former director of the National Security Agency who now runs a cybersecurity firm. The number of sophisticated attacks is growing, he said. “There is a constant, steady upbeat. I see a rising tide.”

No one claims that it would be easy to bring down the grid. To circumvent companies’ security, adversaries must understand the networks well enough to write code that can communicate with tiny computers that control generators and other major equipment. Even then, it’s difficult to cause a widespread blackout because the grid is designed to keep electricity flowing when equipment or lines go down, an almost daily occurrence that customers never see.

Because it would take such expertise to plunge a city or region into darkness, some say threats to the grid are overstated – in particular, by those who get paid to help companies protect their networks. Still, even those who said the risks of cyber threats can be exaggerated agree it is possible for cyberattackers to cause a large-scale blackout.

Traditional central power stations and transmission systems include equipment that is decades old and physically unable to handle electronic threats. Some run on machines that use software that is so old that malware protections don’t exist, such as Windows ’95 and FORTRAN, a programming language developed in the 1950s.

At the Tennessee Valley Authority, a corporation owned by the federal government that powers 9 million households in the

southeastern U.S., a former operations security expert said in recent years he saw passwords for some key operating systems stored on sticky notes.

“Some of the control systems boot off of floppy disks,” said Patrick Miller, who has evaluated hydroelectric dam cybersecurity for the U.S. Bureau of Reclamation and Army Corps of Engineers. “Some dams have modeling systems that run on something that looks like a washing machine hooked up to tape spools. It looks like the early NASA stuff that went to the moon.”

The rush to tie smart meters, home programmable thermostats and other smart appliances to the grid also is causing fresh vulnerabilities.

About 45 percent of homes in the U.S. are hooked up to a smart meter, which measures electricity usage and shares information with the grid. The grid uses that information to adjust output or limit power deliveries to customers during peak hours.

Those meters are relatively simple by design, mostly to keep their cost low, but their security is flimsy. Some can be hacked by plugging in an adapter that costs \$30 on eBay, researchers say.

FERC recently raised concerns about another area that is not covered by federal cybersecurity rules: contractors that sell energy companies software and equipment. As is evident from the Calpine incident, attackers have used outside companies to pull off hacks against energy companies.

“We’ve got these vulnerable systems out there that are old and never had security built into them, and now we’re exposing them to a wider audience,” said Justin Lowe, a utility cybersecurity expert at PA Consulting Group.

“That wider audience is getting much more hostile.”

The full extent of the attacks on the grid is not public knowledge. A Freedom of Information Act request by the AP for information regarding any FBI investigations of such hacks was not fulfilled. The Department of Justice said that agency kept no record of how often any such cases had been prosecuted.

The North American Electric Reliability Corporation, which oversees the reliability of the electrical sector, collects information about cyber incidents involving utilities and other users, owners, and operators of the bulk power system – but it is scrubbed of identifying information and details are confidential and exempt from disclosure under FOIA.

Authorities say they take the threat seriously. In response to a FOIA request, Homeland Security said it had helped more than 100 energy and chemical companies improve their cyber defenses, and held both classified and unclassified briefings in June 2013 and late 2014 on threats to companies associated with power grid operations.

A small DHS team compiles statistics about hacks and vulnerabilities on control systems powering the grid and other public infrastructure, and responds to some attacks. But former federal employees who spoke on the condition of anonymity because the information was sensitive said government red tape kept the team from thoroughly responding to the smaller municipal and rural utilities that most needed their help, and that the statistics overstated the agency's grasp of the problem.

The companies themselves say they are vigilant – though they caution no fortifications are foolproof.

Early this year, an operations supervisor in Virginia for a subsidiary of American Electric Power – the nation's largest power grid operator, with operations in 38 states – opened a personal email on a company laptop and unwittingly downloaded a piece of malware called CryptoLocker.

Known as “ransomware,” CryptoLocker is a relatively common type of malware that reaches to outside servers, usually overseas, and downloads encryption instructions that scramble a computer’s contents, making them inaccessible to anyone without a specific “key.” The malware then moves through a computer – and computer network – and encrypts all the files it can, keeping users from accessing anything.

In exchange for a fee, the hackers provide the victim a key that allows the files to be unlocked.

Members of AEP’s cyber-security team – housed in the company’s Columbus, Ohio, headquarters behind an unmarked door that unlocks with a fingerprint scanner – saw the strange network behavior as soon as it started.

“When you see this (code) attempting to hit thousands of systems outside of the AEP network, that’s a ‘holy crap’ moment,” said Sean Parcel, AEP’s lead cyberinvestigator.

Had CryptoLocker wormed its way into AEP’s system, the business and operations networks could have locked up, experts say.

But Parcel said AEP’s cyber team already had blocked the foreign addresses that the malware needed to reach to start encrypting files, part of a policy of systematically blocking hundreds of Internet Protocol addresses each week to keep employees from inadvertently downloading malicious code.

AEP said the team remotely isolated and erased the supervisor’s computer before its systems were affected.

Like most big utilities, AEP’s power plants, substations and other vital equipment are managed by a network that is separated from the company’s business software with layers of authentication, and is not accessible via the Internet. Creating that separation, and making sure that separation is maintained, is among the most important things utilities can

do to protect the grid's physical assets.

But cybersecurity experts say the protective gaps between computer systems that manage utilities' business operations and machines that manage their grids are not always as wide or as unbridgeable as utilities say they are. And even the utilities' own experts, who maintain it would be extraordinarily difficult for a hacker to knock out power to customers, admit there is always a way in.

"If the motivation is high enough on the attacker side, and they have funding to accomplish their mission," Parcel said, "they will find a way."

Gas prices still falling

By Associated Press

The price of gasoline nationwide keeps dropping.

Industry analyst Trilby Lundberg said Sunday the average price of regular gas fell 4 cents in the past two weeks, to \$2.06 per gallon. That's the lowest price since April 2009.

But the price-tracking website GasBuddy.com says the average has dropped to \$1.99 per gallon, the first time it's been below \$2 since March 2009.

Prices have dropped because supplies are strong and demand hasn't been huge. GasBuddy predicts that many areas will see low prices for much of the winter, although refinery issues in the West could drive prices up.

Gas has fallen below \$2 in 30 states, and more than two thirds of U.S. gas stations are selling at \$1.99 per gallon or less,

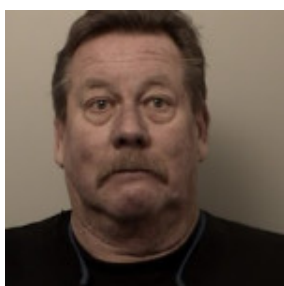
according to GasBuddy. The website says the national average could bottom out at \$1.85 before rising in the spring as demand rises and refineries shift to federally required summer gasoline blends.

Lundberg says the average cost of midgrade is \$2.35 per gallon, while Premium averages \$2.55.

In California, where prices are highest, she says a gallon of regular averages \$2.61, with midgrade costing \$2.74 and premium at \$2.83.

In the Lower 48 states, the highest average price of regular gasoline is in Los Angeles, at \$2.71, while Tulsa, Oklahoma has the lowest, at \$1.72, according to Lundberg.

West Slope fire chief resigns



William Dekker

Garden Valley Fire Chief William Dekker resigned today, five days after his latest arrest on DUI charges.

Details of the separation have not been released.

The board of directors for the West Slope fire district met

Dec. 22. They appointed Linda Szczepanik as interim chief. Dekker was **pulled over Friday** afternoon. This was not his first alcohol related arrest.

– Lake Tahoe News staff report

Peregrine falcons on the rise in Tahoe

Publisher's note: *This article first appeared in Tahoe In Depth and is reprinted with permission.*

By Will Richardson

It's August at Lake Tahoe, the peak of shorebird migration, and the low water level means ample beach and mudflat habitat at the delta formed by the Upper Truckee River and Trout Creek.

Sandpipers and plovers of a dozen species are spread out along the beach, feverishly fueling up for the next leg of their southbound journey, when suddenly – panic. The birds alight, coalescing into a swirling aerial ball, fragmenting and reorganizing. The swarm stretches and splits into two groups as a peregrine falcon slices straight through the middle of the flock, plucking an indecisive straggler along the way. It's a thrilling spectacle, but less common at Tahoe until recent years.

The peregrine's name means "wandering falcon" and it has the most extensive natural range of any bird species on the planet. Prior to the Comstock era, it is likely that peregrine falcons were regular breeders in, and certainly would have

been regular migrants though, the Lake Tahoe region. An 1877 report by the U.S. Geological Survey describes the species as “met with frequently in early fall.”

As recently as the early 1940s, peregrines were known to nest at Echo Summit and Cave Rock, but over the course of the next several decades, the species experienced precipitous population declines around the world due to the use of organochlorine insecticides like DDT, aldrin, and dieldrin.



A peregrine falcon eats a band-tailed pigeon near Sand Harbor. Photo/Will Richardson

The approximately 3,875 breeding pairs of peregrines in North America prior to the 1940s declined to 324 breeding pairs at their lowest point in 1975. DDT use was banned in the U.S., Canada, and most of Western Europe by the early 1970s, but it

took many years to bring the species back from the brink.

One method used to promote rapid population growth and expansion was captive breeding and hacking. Nestling birds hatched from captive breeding programs (often involving falconry birds in the case of peregrine falcons) were reared in a wooden box to help protect them from predators and weather, and these boxes were placed at unoccupied but otherwise suitable nesting sites, typically a high cliff, a couple of weeks prior to fledging. Once the birds had been at the site for five to 10 days, the box was opened, giving these birds the freedom to move around the site, flap their wings, and build strength.

Biologists provided the birds food throughout the hacking process, but there was minimal contact and biologists often used hand puppets to simulate feeding behavior of adult birds. From 1985 through 1991, 18 juveniles were released at two hack sites in Tahoe, one at Luther Rock and one at Eagle Falls. All 18 birds successfully fledged and dispersed, and the program was considered a success, though where these birds ultimately dispersed to is anybody's guess. Migrants and presumed transients would steadily increase during the 1990s and 2000s, but it was 22 years since the last hacking effort at Luther Rock before peregrines were confirmed to be breeding again at Lake Tahoe.

In 2007, peregrine falcons were observed in late summer near both South Maggies Peak and Angora Peak. Further investigations revealed that a rock-climbing biologist had observed a peregrine at Luther Rock in 2006. In 2008, the wildlife crew of the U.S. Forest Service Lake Tahoe Basin Management Unit began monitoring potential nesting sites based on a 1980 nesting survey, and the following year a nest was found at Luther Rock.

What's more, the pair at that nest successfully fledged two young. By 2011, a second nest was discovered at Castle Rock.

In 2014, a third nesting pair was confirmed at Cave Rock, and this summer a fourth nest was found at Eagle Lake. Thanks to heroic efforts on a shoestring budget, the wildlife crew at LTBMU has managed to confirm that each of these locations has remained active since they were first found, typical of the species, and a minimum of 20 juveniles has fledged at Lake Tahoe over the last seven years. This is truly an impressive rebound for the peregrine.

Birders and biologists rejoice at the return of the peregrine to Tahoe. Their great speed and hunting skill can be exhilarating to observe. As Forest Service biologist Shay Zanetti points out, "they add an exciting element to the basin ecology." But perhaps more importantly, they belong here.

Now we need to make sure we can sustain all of these breeding predators, and foraging habitat may prove limiting. Peregrines prefer to hunt water birds and were once known as "Duck Hawks" in this country.

Prior to the construction of the first dam at Tahoe City in the 1860s, there was far more shorebird and wetland habitat distributed around the lake's shoreline. Extensive beaches and mudflats were perhaps more consistently available from year to year. Now the best waterfowl and shorebird habitat has been reduced and concentrated into a few small pockets, especially when the lake is full.

Thus, we need to consider the peregrine falcon, perhaps nesting miles away on some craggy cliff side, when setting policy that can affect the bird population at a given location. That's why it's important for dog owners to keep their pets on a leash at the Upper Truckee Marsh or many of Tahoe's beaches. But it also applies to forest management practices that might affect band-tailed pigeons, Steller's jays, Northern flickers, or other birds the peregrine relies on for food. To support a healthy population of peregrine falcons at Lake Tahoe, we need healthy populations of the

other bird species as well. Based on the recent trajectory of peregrine recovery at Tahoe, it appears things are looking up.

Will Richardson is co-founder and co-executive director and director of applied science at the Tahoe Institute for Natural Science.

Letter: Homeless Coalition grateful for support

To the community,

On behalf of Tahoe Coalition for the Homeless, I would like to thank our community for a successful opening of the South Lake Tahoe Warm Room.

Peggy Eichorn and Kelly Pelcher from Coldwell Banker McKinney were instrumental in the search for a location for the Warm Room, and have been an unwavering partner in the project. We thank them for their support. Also, the coalition is grateful to Star Lake Investments for use of their facilities.

We also appreciate those who helped make the South Lake Tahoe Warm Room safe for overnight guests. Rob Worth, Jim Pelcher, and Erik Finkelstein of Innovative Electric donated labor in order to complete our building upgrades. Dan Graham at Tahoe Valley Electric donated supplies as well. South Lake Tahoe is very fortunate to have individuals and businesses like these supporting nonprofit efforts such as ours.

Over 40 individuals and 10 partner agencies have come together to provide short term assistance to our friends and neighbors who find themselves without housing this winter, and to

provide resource referrals to help break the cycle of homelessness.

Tahoe Coalition for the Homeless is still looking for more volunteers to assist during the 2015-16 winter. Three training sessions are scheduled next month: Jan. 9 from 10am to 12:30pm; Jan. 12 from 1pm to 3:30pm; and Jan. 12 from 6pm to 8:30pm. If you are interested in becoming a volunteer, please contact Tahoe Coalition for the Homeless at tahoewarmroom@gmail.com or 775.573.0822.

Donations are also welcomed to aid in funding the Warm Room. Checks can be made payable to Live Violence Free (Tahoe Coalition for the Homeless' fiscal sponsor), note "Warm Room" in the memo line and mail to P.O. Box 13514, South Lake Tahoe, CA 96151.

Marissa Muscat, Tahoe Coalition for the Homeless

Lake Tahoe and snow base keep rising



Lake Tahoe Rises 1.92 Inches in Latest Storm

Just how much water is that?

- The graph at the right shows how the water level has risen on Lake Tahoe since midnight Dec. 21st
- This is 0.16 feet or 1.92 inches.
- Here is the volume of water this equates to
 - 19600 Acre-feet
 - 63.9 Billion gallons
 - 242 Billion Liters
- That's a LOT of water!



Motorists are now able to get over most mountain passes in the Lake Tahoe area.

Earlier this morning a slide closed Highway 50 over Echo Summit. Caltrans has cleared it. Highways were a mess last night, with most of them closed at times. It was taking motorists double their normal drive time and then some to get to their destinations.

Highway 89 around Emerald Bay is closed.

Crews were out doing avalanche control, as the booms resonated through neighborhoods. This was to make the roads safe.

The Sierra Avalanche Center is saying the danger level for Dec. 22 is "considerable". This is for below, at and above tree line.

The National Weather Service in Reno has issued a flood warning until 4pm Tuesday for the burn areas including the

King Fire that scarred the forest near Pollock Pines. The warning also includes the Rim, Butte and American fire locations.

The good news about the rain at lower elevations is that Lake Tahoe has risen 1.92 inches in the last storm, according to the National Weather Service. The agency said 4.3 billion gallons of water fell in to the lake in a 30-hour period.

Most of the ski resorts are reporting 10 inches or more of snow. Sierra-at-Tahoe and Tahoe City Cross Country closed on Tuesday to dig out.

More snow is in the forecast for the rest of the week, with 100 percent chance on Thursday.

For current road conditions, click on the state icons on the home page of *Lake Tahoe News*.

– *Lake Tahoe News staff report*

Snippets about Lake Tahoe



• BlueGo is offering free rides on some routes from now until Jan. 3. For more info, go **online**.

• South Lake Tahoe clears the class 1 bike paths when 3 or more inches of snow have fallen. In an effort to evaluate the costs for the services, the city is asking people to take this **survey**.

- Disabled Sports USA Far West, a nonprofit organization providing specialized sports instruction for people with physical, sensory and intellectual challenges has changed its name to Achieve Tahoe.

- East West Resorts based in the Vail Valley is now East West Destination Hospitality. In Lake Tahoe, the company offers a variety of North Lake Tahoe vacation rentals, including luxury residences in the Village at Northstar and at Old Greenwood.

- Natasha Shue, publisher of the *Tahoe Daily Tribune*, is leaving in January to work in Barton Health's marketing department.