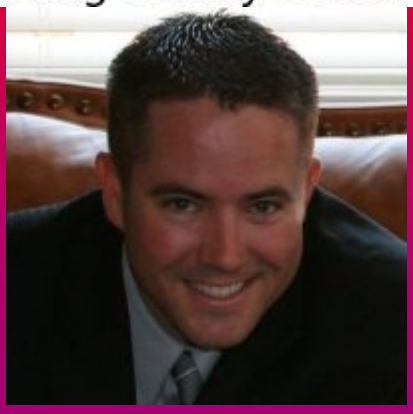
NORTHERN NEVADA ASIS INTERNATIONAL
CHAPTER #164

January 4th, 2016
Volume 6, Issue 3

Security Vanguard



Mark Crosby, CPP

Chairman's Corner

Happy New Year! I hope everyone had a very safe and enjoyable Holiday season. The family and I spent the week before Christmas in a cabin outside of Yosemite this year. The weather cut our vacation a little short, but it was a great break from the action while it lasted. Back to work!

Last month we held our annual Law Enforcement Appreciation luncheon. I want to thank everyone for your participation in that event this year which was once again sponsored and hosted by the Atlantis Casino Resort. Thanks to Atlantis for their generous support of ASIS and our law enforcement partners. Dean Hill did a fantastic job again this year, and the event was very well received. GREAT WORK DEAN! I'd also like to give special thanks to our other event sponsors including Al Zajic of AWZ Consultants, Jason McLean with Charter Communications, Chris Brockway with the Nugget, Darrell Clifton with the Reno Circus Circus, Mike Hendi of ESI Security and Shred It, Kevin Schaller of Resiliency Partners, Sharon Oren of Maccabee Arms, Jes Stewart with the Nevada Museum of Art, Cliff Hufnagle of NV Energy, Dean Hill of the Peppermill, Dave Gish of RFI Communications, Guy Hyder of the Silver Legacy and Joe McDonald of Switch Supernap. I sincerely appreciate your gen-

Cont. Page 2.

Inside this issue

erous contributions. You and your companies made this another especially meaningful event for our law enforcement honorees.
With 2016 now upon us, I look forward to another great year for the chapter. We have some of the most knowledgeable and competent security

As another year presents itself with all of its possible opportunities to learn and enjoy ourselves, so does it present the possibility of risk. There are both tangle and intangible risks that present themselves every day throughout the year. Keeping up with the current trends of individuals with malicious intent can be invaluable to us, to our friends and families, to our individual places of employment, and to the security industry as a whole.

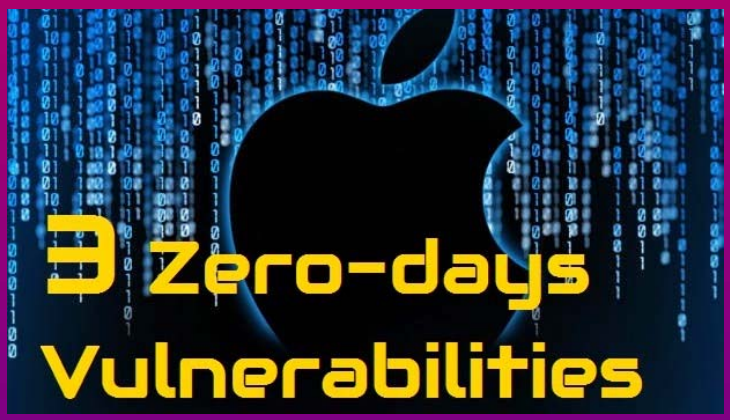
15 Cybersecurity Lessons We Should Have Learned From 2015, But Probably Didn't

Another InfoSec year is almost in the books. What did all the breaches, vulnerabilities, trends, and controversies teach us?

1. Pay For Your Room In Cash.
Retailers were in hit hard in 2014, but in 2015 point-of-sale hacks really moved over to the hospitality sector. Just Thursday, Hyatt Hotels announced it was the last to be breached (it had discovered the incident Nov. 30). Before that Hilton Worldwide, Mandarin Oriental, and Starwood Hotels & Resorts (the owner of Sheraton, Westin, and W Hotels) all suffered breaches due to similar attacks. It isn't just credit card data that is appetizing to attackers, either. Info about loyalty programs is hot on the black market, too.

2. Take The Train Instead.
This was the year when car hacking really got taken seriously. Security researchers Chris Valasek

and Charlie Miller conducted a controversial demonstration taking remote control of a Jeep Cherokee and bringing it to a screeching stop. The Virginia State Police showed their cruisers could be compromised and researchers showed SMS messages sent to insurance dongles can kill brakes on cars. The issue got so unavoidable that Chrysler recalled 1.4 million vehicles and Intel founded a Car Security Review Board.



3. Trust Apple, But Not As Much.
Although security researchers agree that the state of Apple security is still far better than Android, but the trusted development environment took some serious hits this year. XCodeGhost snuck Trojanized iOS apps into the official App Store, a variety of proof-of-concept exploits in Gatekeeper allow unsigned code to run on OS X, and malware for iOS and Mac is increasing.

4. The Encryption Backdoor Debate Is Not Going Away.
The U.S. intelligence agencies may have retreated periodically -- backing off on demands for encryption backdoors, and focusing instead on end-to-end encryption -- but that doesn't mean the conversation is over. With every new terrorist act, the threat of having liberties and privacy taken away becomes greater, and the encryption discussion has even become part of Presidential debates.

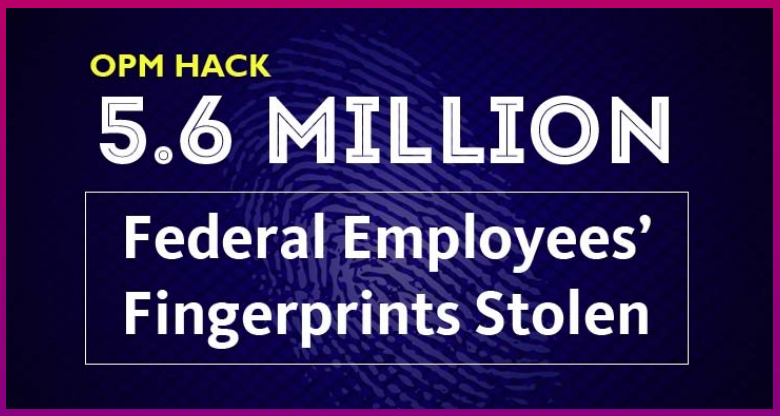
5. Don't Get Sick.
Over the past 10 years, more than one-quarter of reported data breacheshappened in the healthcare industry, according to Trend Micro. This year, the PHI exposures at medical insurers were of gobsmacking dimensions -- 10 million records exposed by Excellus Blue Cross Blue Shield (BCBS), 11 million by CareFirst BCBS, 11 million by Premera BCBS, 250,000 by LifeWise, and a stomach-turning 80 million from Anthem Healthcare.

6. Exporting Exploits and Hoarding 0-Days Are Bad...Unless You're A Govern-

http://www.calea.org/calea-update-magazine/issue-101/police-training-officer-pto-program
Website Title: A New Strategy for Training Police Officers
Article Title: A New Strategy for Training Police Officers - the PTO Program

ment.
Proposed updates to
the Wassenaar Arrangement this year (which are getting another look, thanks to the advocacy efforts of security professionals) would put tight restrictions on US companies' ability to export "intrusion software" internationally. Yet, the breach of Italian surveillance companyHacking
Team revealed that many government agencies, including the FBI, purchased surveillance, exploit tools, and zero-day vulnerabilities from the firm. An FBI official recently publicly admitted that the Bureau buys zero-daysand
the NSA says it discloses 90 percent of the vulnerabilities it finds, but didn't reveal how quickly it does so.

7. Flash Will Survive The Apocalypse.
Adobe Flash has been riddled with critical vulnerabilities this year, including some zero-days revealed in the Hacking Team leaks. US-CERT released an advisory, Mozilla stopped running Flash by default, and Facebook's security chief demanded Adobe announce a date of-death for Flash. Yet, the technology persists. So, Flash is in the same category as cockroaches and ticks. Everyone wants them to die, but try as they might, they just can't kill them. So, really, if you want your manifesto to still be viewable after the collosal supervolcano or sentient robot uprising, build it in Flash.

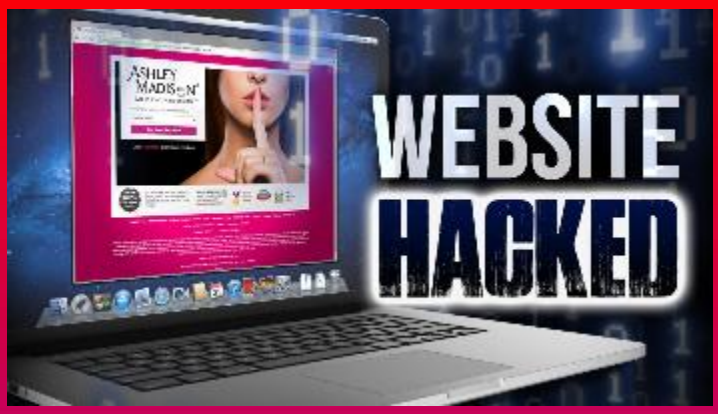


8. Government Jobs Aren't Really So 'Secure'.
The breach at the U.S. Office of Personnel Management resulted in the exposure of personal data on anyone who's had a background check via OPM going back to the year 2000. In all, 21.5 million people's Social Security numbers, residency and employment history, family, health, and financial history as well as fingerprints

on 5.6 million people were exposed.

9. Keep Backups. No, Really.
Ransomware was everywhere in 2015, and there's no reason to expect its growth will stop or slow down. Research found that ransomware use was growing, the malware itself was growing more sophisticated, the business models were becoming more varied, it had an exceptionally high return on investment, and many targets were helpless against it. Even several police departments simply paid up when they couldn't recover their assets any other way.

10. Extortionists Have More Than Ransomware At Their Disposal.
In addition to the criminals using ransomware to extort money from victims, there are bad guys gathering their Bitcoins
from DDoS, doxing, or other cyber-enhanced blackmail threats.
The Ashley Madison breach gave extortionists, blackmailers, and the average unscrupulous capitalist plenty of opportunities to collect.



11. Manage Privileged Users Better.
Study, after study, after study this year revealed that privileged accounts need to be better managed. It isn't just that the credentials themselves are too weak, but sometimes they're poorly monitored, too widely shared, and they're not efficiently revoked when employees leave an organization.

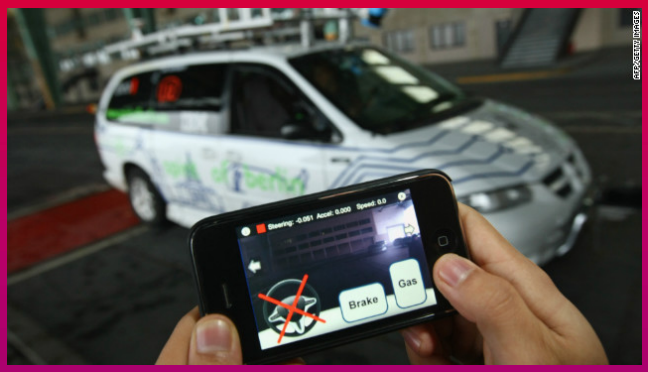
12. Watch Out For Insiders.
Another reason to manage privileged accounts is that not all who are privi-

ASIS INTERNATIONAL
Advancing Security Worldwide®

leged are trustworthy. 2015 kicked off with news that Morgan Stanley fired a wealth advisor who accessed data on about 10 percent of its client roster and publicly posted details for 900 of them online.

13. Start Making Friends at the FTC.
The Third U.S. Circuit Court of Appeals ruled that the U.S. Federal Trade Commission could move forward with its lawsuit that alleged Wyndam Worldwide hotel chain should be held responsible for leaving its customer data unprotected. The ruling effectively gives the FTC the power to regulate the security practices of businesses.

14. Everyone Could Be A Target Of Cyber Espionage.
Whether it's the St. Louis Cardinals hacking the Houston Astros,cybercriminals attacking Kaspersky Lab to stay ahead of their threat intelligence, or operators of a shadowy illegal online gambling businesshacking their third-party software provider to make sure their work for a competing gambling company wasn't a threat to their business, the takeaway is that cyber-espionage can happen to anyone.



15. Beware The Thing.
Cars and drones, Fitbits and smart fridges, baby monitors and Hello Barbie, satellites and smart cities...security vulnerabilities were found all over the Internet of Things this year. The coolest hacks this year were all at that intersection between the physical and the virtual and the FBI even came out with a warning about the cybersecurity risks of IoT devices. Luckily, new organizations are arising to try to fix IoT security before it gets completely out of hand.

Sara Peters
15 Cybersecurity Lessons We Should Have Learned From 2015, But Probably Didn't (Dark Reading)
http://www.darkreading.com/attacks-breaches/15-cybersecurity-lessons-we-should-have-learned-from-2015-but-probably-didnt/d/d-id/1323704

LAW ENFORCEMENT APPRECIATION

Presented by ASIS International, Chapter #164
Sponsored by the ATLANTIS CASINO RESORT SPA

Opening Remarks— Mark Crosby — Chapter 164 Chairman

Emcee—Dean Hill - Chairman LEA Committee, Chapter 164

Presentation of Colors—Sparks Police Department Color Guard

Deputy Carl Howell—Carson City Sheriff's Office

Invocation—Chaplain Mark Morton

Keynote Speaker— Chuck Allen— Washoe County Sheriff

Award Presentations to Recipients from the Following Agencies
(In alphabetical order)

Carson City Sheriff's Office
Douglas County Sheriff's Office
Lyon County Sheriff's Office
Nevada Department of Corrections
Nevada Department of Public Safety,
Highway Patrol Division
Nevada Department of Public Safety,
Parole & Probation Division
Reno Police Department
Reno Tahoe Airport Authority Police Department
Sparks Police Department
Storey County Sheriff's Office
University of Nevada Police Services—Reno Division
Washoe County School District Police
Washoe County Sheriff's Office

Closing Remarks:—Dean Hill

LAW ENFORCEMENT APPRECIATION

CONGRATULATIONS TO ALL RECIPIENTS!!

2015 Award Presentations

Carson City Sheriff's Office
Recipient: Deputy John Hitch

Douglas County Sheriff's Office
Recipient: Investigator Jon Storke

Lyon County Sheriff's Office
Recipient: Deputy Jeremy Best

Nevada Department of Corrections
Recipient: Criminal Investigator Darin Baker

Nevada Department of Public Safety, Highway Patrol Division
Recipient: Trooper Karen Garretson

Nevada Department of Public Safety, Parole & Probation Div.
Recipient: Officer Richard Linnenbrink

Reno Police Department
Recipient: Officer Santiago Santiago

Reno Tahoe Airport Authority Police Department
Recipient: Sergeant Ray Guzman

Sparks Police Department
Recipient: Officer Ben Russell

Storey County Sheriff's Office
Recipient: Deputy Renee Deitrick

University of Nevada Police Services—Reno Division
Recipient: Officer Robyn Wasser

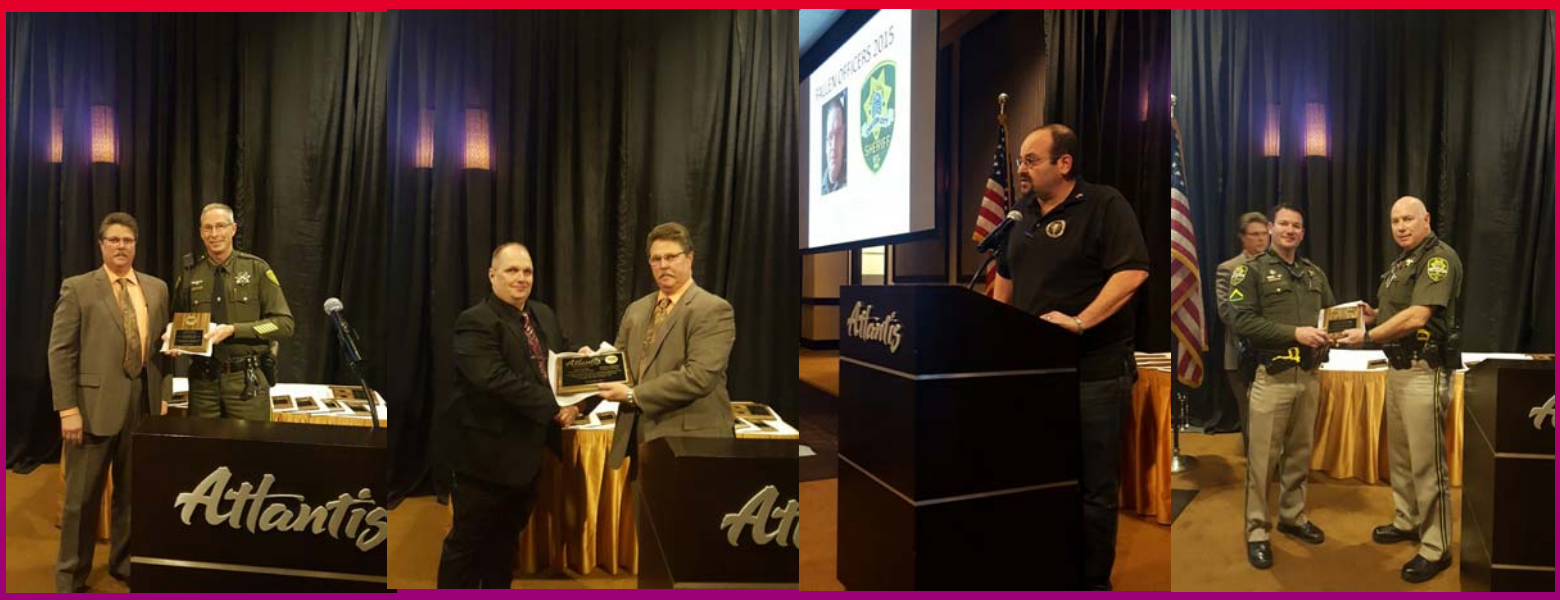
Washoe County School District Police Department
Recipient: Detective Bruce Hobbs

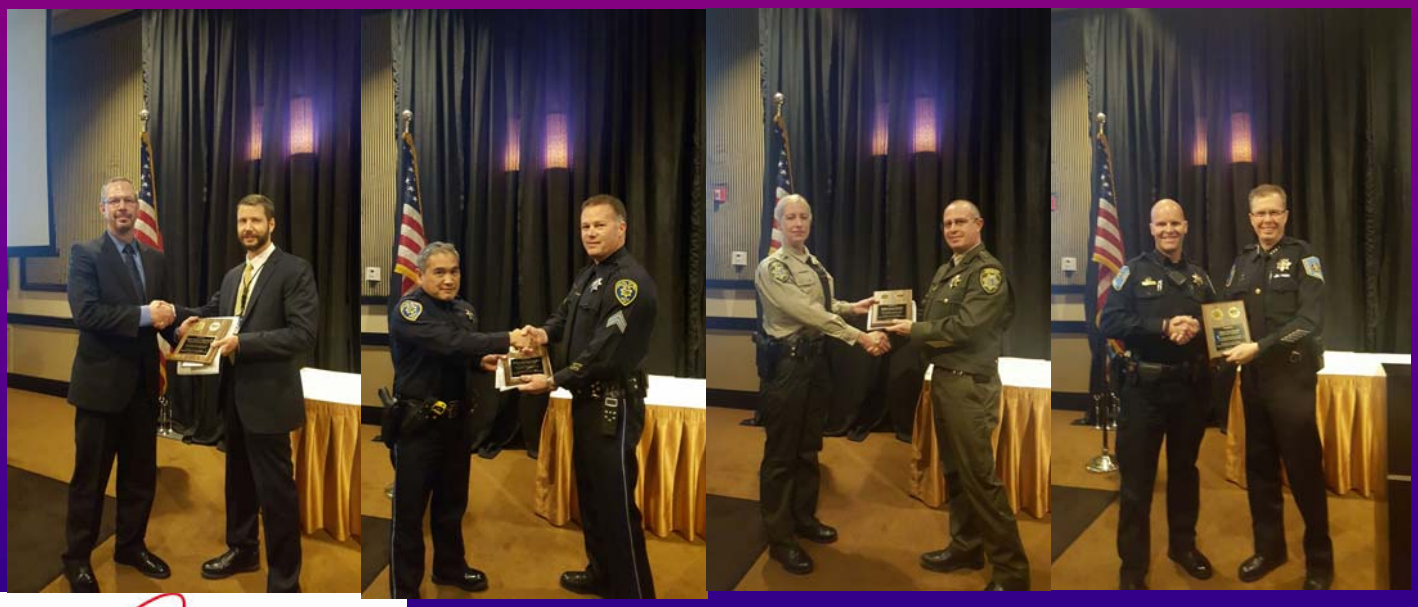
Washoe County Sheriff's Office
Recipient: Deputy Jeffrey McCaskill

So thank you to everyone who was able to attend the Law Enforcement appreciation ceremony, and hear some real inspirational stories. It's sad the way the media portrays Law Enforcement Officers who sacrifice their time, and even their lives to keep us safe. We appreciate and owe our comfort and continued safety to you. Keep safe and thank You!!

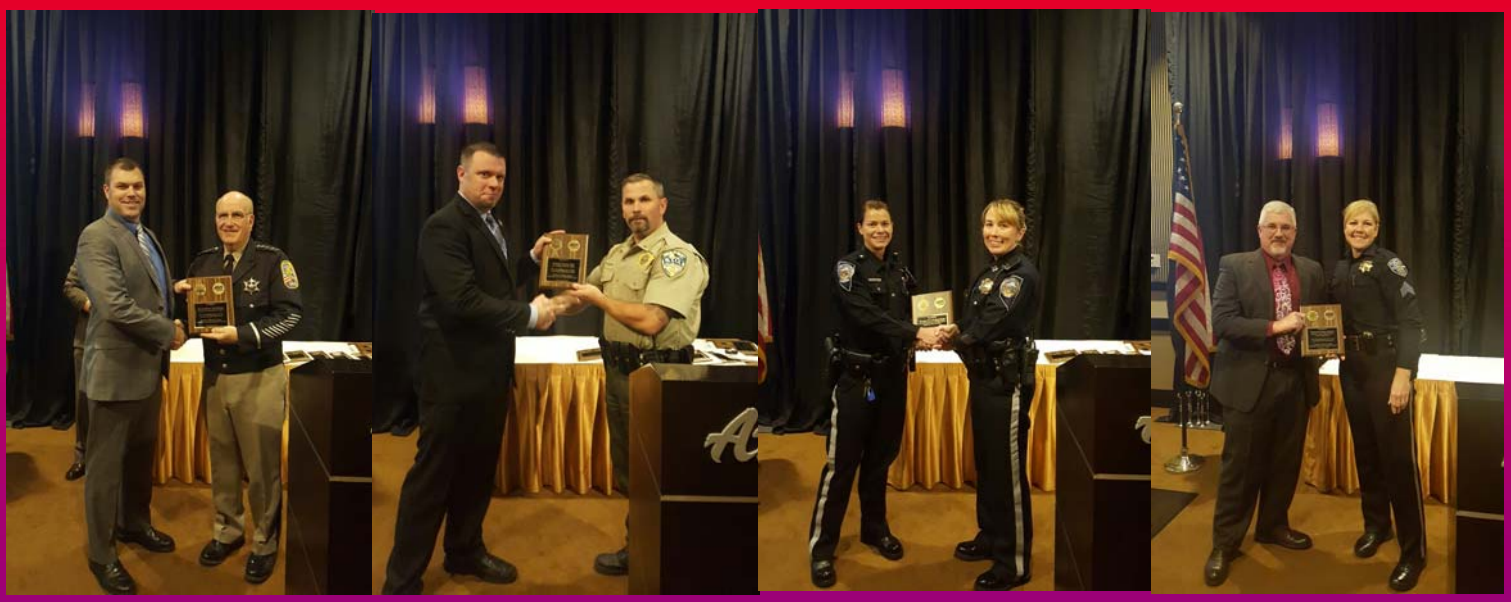
ASIS INTERNATIONAL
Advancing Security Worldwide®

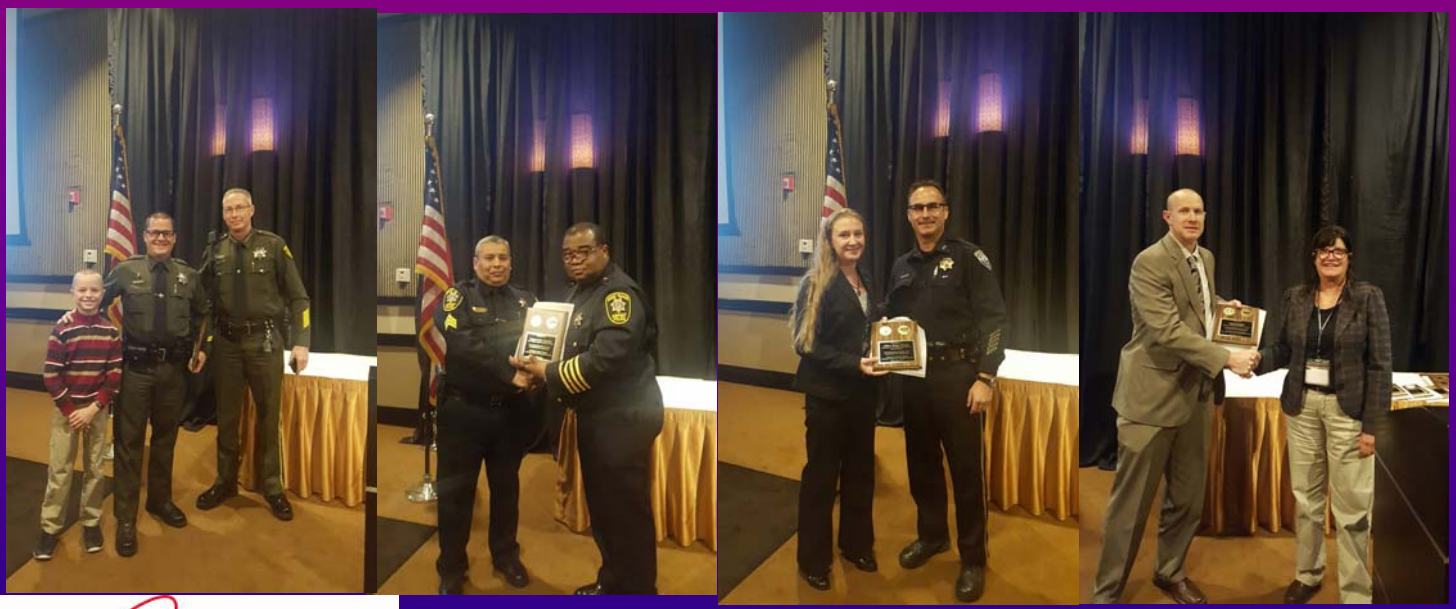
Law Enforcement Appreciation Pictures





Law Enforcement Appreciation Pictures





ASIS INTERNATIONAL
Advancing Security Worldwide®

Please be advised Future webinars will be offered and notifications will be sent out regularly.

If you feel you are not receiving these notifications please notify Mark Crosby

ASIS Chapter #164

Where: Innevation Center

450 Sinclair St, Reno, NV 89501

Date: Wednesday, January 6th 2015

Time: 11:30 AM – 1:30 PM (approximately)

Cost: $20.00 per person

If you have any suggestions about the news letter please contact Michael Smith

Chairman:	**Mark Crosby**
Vice Chairman:	**John Puccioni**
Secretary	**Mike Gach**
Treasurer	**Cliff Hufnagle**
Membership Chairperson	**TBD**
Newsletter Editor	**Michael Smith**
Law Enforcement Liaison	**Dean Hill**
Legislative Rep	**Ken Braunstein**
Chapter Webmaster	**John Puccioni**
ASIS Foundation Rep	**TBD**
Scholarship Chairman	**Ken Braunstein**
Chapter Photographer	**Ken Braunstein**
Audit Chair	**Ken Lightfoot**
Certification Rep	**TBD**
Young Professionals Liaison	**TBD**
Women In Security	**TBD**

ASIS INTERNATIONAL
Advancing Security Worldwide®