NORTHERN NEVADA ASIS INTERNATIONAL
CHAPTER #164

February 1st, 2016
Volume 6, Issue 4

Security Vanguard

Mark Crosby, CPP

Chairman's Corner

I'm writing this month's Chairman's Corner after having narrowly escaped Winter Storm Jonas, which ravaged the east coast just after the Annual ASIS Leadership Conference in Washington DC. I had two flights cancelled out of Dulles, and as I understand it was just minutes away from being asked to debark we ultimately made it home on time. Good times, but I'm glad to be home.

This was my first time attending the ASIS Leadership meeting in DC, and it was a great experience for me. I had an opportunity to hear from our new President, David Davis, CPP, as well as from our newly named EVP and CEO, Peter O'Neil, and was impressed with each. Although it was made clear that there will be many challenges faced by our organization in the coming years, it was also clear to me that we have some very intelligent and motivated people serving as volunteer leaders, and a very competent staff at headquarters making sure we execute on our missions and overcome adversity.

I want to take a moment to thank Ken Lightfoot and Scolari's Food and Drug for graciously hosting our most recent ASIS Webinar, entitled The Future Effects of Rapid Security Technology Change. There was some very interesting material covered by a group of top notch professionals who were thought leaders in the security and IT industry. I personally received some great insight into future trends in security technology and how deploying and even operating security technology may change in the future.

I look forward to seeing you at our next meeting being held Wednesday, February 3rd at the UNR InNevation Center, where our guest speaker will be Special Agent David Linterman with the Federal Bureau of Investigation. Please come out to join us.

Inside this issue

Chairman's Corner..........................1

ISIS: The Threat to the United States

ThreatKnowledge.org 2-3

10 tips to secure your small business network.......................................4-5

Meeting Minutes 6-7

ISIS: The Threat to the United States

ThreatKnowledge.org

November 2015

With the November 13th attack in Paris that killed 130 people and injured 368, many are asking what the risk is of a similar attack on U.S. soil. While France has a proportionately larger Muslim population than the United States (7.5% of the total population in France compared with .6% – 2.2% in the U.S.), ISIS has already recruited supporters in the United States with the intent of executing domestic attacks here in America. Key evidence includes the following:

82 individuals in the United States affiliating with ISIS have been interdicted by law enforcement since March 2014 (including 7 unnamed minors and 4 killed in the course of attacks). (For a full list of those individuals see www.ThreatKnowledge.org)

More than 250 individuals from the United States have joined or attempted to join ISIS in Syria and Iraq according to the Final Report of the Task Force on Combating Terrorist and Foreign Fighter Travel published by the U.S. House of Representatives Homeland Security Committee in September 2015.

The FBI currently has nearly 1,000 ongoing ISIS probes in the United States, according to a recent report by Judicial Watch.

ISIS is recruiting within the U.S. at about three-times the rate of Al Qaeda.

Ali Shukri Amin, a 17 year-old Islamic State (IS) supporter from Manassas, Virginia, recently sentenced to 11 years in prison for conspiring to provide support to ISIS, had nearly 4,000 Twitter followers, under the alias, ‘Amreeki Witness.’

Ahmad Musa Jibril, an Arab-American Islamist preacher living in Dearborn, Michigan, had 38,000 Twitter followers before his site went silent. A report by the International Centre for the Study of Radicalization (ICSR) found that 60% of surveyed foreign fighters in Iraq and Syria followed Jibril on Twitter.

ISIS is a fully-fledged insurgency, not merely a terrorist group as Al Qaeda was. Wherever it had been operating over the last 14 years, Al Qaeda was never a true insurgency. For example, in both Afghanistan and Somalia it functioned as a terrorist organization which attached

itself to a pre-existing domestic insurgency, the Taliban and Al Shabaab respectively. In these theaters Al Qaeda never recruited its own mass base of fighters. In contrast, in less than two years ISIS has recruited an insurgent force of indigenous and foreign fighters that now numbers more than 60,000. As a result, it has been able to successfully capture large expanses of territory in multiple countries, giving it far greater reach and recruiting capability than Al Qaeda ever had.

How should the United States respond to this heightened threat environment?

Stop downplaying the seriousness of the threat so that individuals and law enforcement can be properly prepared.

Recognize that ISIS is targeting youth, and do more to protect youth from radicalization. Educate those who work with youth about the indicators of radicalization. Hold parents criminally liable for not preventing their children from supporting ISIS where it can be established that they were aware of it.

Target the ideologues. Recognize the link between rhetoric that calls for death of the infidel and acts of terrorism and interrupt the flow of such communication.

Better utilize open-source intelligence. Both domestic supporters as well as ISIS-central and Iraq and Syria are boldly announcing their plans and intentions. Law enforcement should take that intelligence seriously and act on it.

Screen refugees. While accepting those who flee from persecution and violence is a valued component of the American tradition, we must acknowledge that ISIS and other terrorist groups may use the refugee track as a way to gain access

The United States, indeed the world is facing a threat unlike any it has seen. The old rules of engagement no longer pertain, and terror is the order of the day. Citizens are as vulnerable (if not moreso) than soldiers. If we want to prevent the loss of more lives we must acknowledge the seriousness of this threat. That does not mean making Muslims register or banning all refugees, but neither does it mean continuing with the status quo. There is much that can be done by law enforcement, by intelligence and by citizens to keep America safe and yet also free. We have outlined a few of those steps here as a place to start.

10 tips to secure your small business network

Maintaining a secure small business or home network isn't easy, and even for an old hand in IT, it still takes time and energy to keep things locked down. Here are 10 of the most critical steps you can take to keep your data from ending up elsewhere, and none of them take much time or effort to accomplish.

1. **Use encryption on your wireless access points (AP).**Many site surveys have found half or more of all wireless networks are wide open, ripe for anyone to gather all the traffic and perhaps record your sensitive information by sitting in a nearby parked car. Some people mess around with locking down MAC addresses, but that gets unwieldy and a better solution would be to use WPA2 encryption. WPA2 is far better than other encryption methods that are more easily broken into.

2. If you have a wireless network, **make sure to hide your SSID (service set identifier)**, or at least change its name to something common. All wireless routers should have obscure IDs when they announce themselves to the world. Rather than put in any real information that can make it clear who owns the router or that can divulge your location or business name, such as "Acme Systems, here on the 4th floor" or the product name like "Netgear," use something innocuous like "wireless" or "router1" that doesn't give away anything really critical. In my last apartment, I had neighbors who used their apartment numbers for their IDs, making it real easy to figure out who's router was where.

3. If your router (wired or wireless) has a Web management interface, **disable access from the outside network. And change the admin default password now.** Most routers have the ability to do both quite easily. You don't want anyone else coming in and changing your settings or reading your log files.

4. **Make sure all of your PCs use antivirus software and if you're using Windows, add antispyware protection.** This seems obvious, but it bears restating. And while you are at it, check to make sure that all of your antivirus subscriptions are current. Anything out of date isn't doing you any good. In my support travels, I've found that this is a very common lapse among my neighbors.

5. If you are running a Web server on your LAN, **put it on a DMZ**. If your router doesn't have a DMZ, get a new router. Better yet, move to a collocation facility where someone who knows what he is doing can manage it. Having your own local Web server sounds like a good idea, but is a real security sinkhole, and many cable networks have made it harder to host your own from your home network anyway. So why worry?

6. Speaking of Web servers on the Internet, if you have them, you should **scan regularly for exploits**.

ASIS INTERNATIONAL
Advancing Security Worldwide®

There are many sites that can do this; two of my favorites are SPIdynamics.com and Qualys.com. Also, make sure to keep track of your domain registry and change all of your access passwords regularly. If you update your Web content, don't use FTP or Microsoft's Web page creation tool, FrontPage; instead, find more-secure methods that don't send your access passwords in the clear. You can learn about other ways to protect your Web site at OWASP.org.

7. If your ISP offers such an option, **use a VPN (virtual private network)** for access back to your local LAN or your remote Web server. There are many to choose from, ranging from the free OpenVPN.net to inexpensive but capable ones from SonicWall and Fortinet, which are designed for small business owners.

8. **Disable file/print sharing on everything other than your file server**. You don't need it on each desktop, and that just causes more vulnerabilities. This is particularly important for laptop users: You don't want to be broadcasting your entire file system to everyone around you at the airport or hotel, which is something that I often see when I travel and check for open network shares.

9. **Use whole disk encryption on** all laptops that will ever leave home. You never know when someone will steal your data or break into your car or hotel room and lift the laptop. I like PGP Disk, but there are others that cost next to nothing and provide plenty of protection. If you are in the habit of carrying around USB thumb drives with your data, then use one of the more modern U3 drives that work with Windows and are at least password-protected to keep your data away from others.

10. **Start doing regular off-site backups now.** At least start with making copies of your key customer and business data, and then make sure you cover your personal files, such as family photos and the like. Now is the time to cook up something simple. Burn DVDs and take them home, or make use of one of the online storage vendors such as eVault andAmazon.com's S3. They cost less than $100 a year (Amazon's less than $10 a year) and can save your data in case of fire, theft or just carelessness. If you have two PCs in two different locations, sign up for Microsoft'sFoldershare.com free service to synchronize your data.

Now, there are plenty of other security options that will buy you peace of mind and make it harder for hackers, but these 10 items are easy to implement, don't cost much in terms of your time and money, and will have big security payoffs. Try to attempt one item each week and you'll sleep better at night.

"10 Tips to Secure Your Small Business Network." Computerworld. N.p., n.d. Web. 01 Feb. 2016.
By David Strom

Meeting Minutes January 6, 2016

ASIS Chapter #164
Meeting Minutes
January 6, 2016

American Society of Industrial Security
Secretaries Report

Location: UNR Innevation Center Room #205
Members Present: 19
Guest Present: 1

Call to Order
Meeting called to order at 12:20 PM by Chairman Mark Crosby

Welcome
Chairman Crosby welcomed members and guest he announced that the meeting is a planning meeting and there will not be a speaker.

Committee Reports
No committee reports were given.

Old Business
Chairman Crosby thanked Dean Hill, Darrell Clifton and all of the chapter members that contributed their effort and resources to an outstanding (LEA) Law Enforcement Appreciation Luncheon. He said that the LEA Luncheon was a great success and is the chapters' largest fundraiser. Mark said that the Southern Nevada Chapter requested information and ideas from our chapter to plan a LEA event for the Southern Nevada. We have a great chapter because our members participate. If the entire member contributes just a little our chapter will be even stronger.

New Business
Chairman Crosby said that ASIS National has issued a directive that all chapters report Activity, Goals and Compliance reporting on the Meeting and Event Information Template.

A discussion was held about ASIS Training Webinars. A motion was made to purchase ASIS's $99-webinar subscription for the chapter. The motion was seconded and approved by the membership. Several members have agreed to hold the webinars at there venues. Chairman Crosby said that he will send out information about 2-weeks before the webinars so members can plan and bring their staff and other guest that might benefit from the training. There was a discussion about the possibility of using the webinars as a recruiting tool and or fundraising.

Chairman Crosby discussed the chapters past training seminar. He said past events were successful, well-attended and generated excellent funding and recognition for the chapter. He suggested that the chapter to plan another training seminar.

Chairman Crosby said that both chapter and national dues are now due. Chapter dues are $25.00. Luncheon cost can be paid in person or online by credit card or Pay Pal. He said if members opt to prepay for all of the luncheons, online, in advance, the local chapter dues would be waived. There is a link on the chapters website and on nationals website to pay online.
Chairman Crosby announced that there are several committee positions open that the chapter is looking to fill they are Women in Security, Young Professionals, Membership, Certifications and Foundation.

The chapters June meeting will be dedicated to the Northern Nevada Security Officer and Security Professional of the year. Members should start thinking about possible nominees for the honors.

Chairman Crosby said that in 2016 monthly chapter meetings would be held at a various locations. The board did not want the chapter to get locked into a yearlong contract at one location. In the past the chapter has had to pay for meals based on a minimum guarantee that we made to the Atlantis for a minimum 20-meals. The chapter lost money when attendance was low. He went on to say that the Atlantis has been a great supporter of the chapter and we will continue to have some meetings there. By moving the meeting locations we will benefit by hopefully increasing

Meeting Minutes January 6, 2016

meeting attendance and members will be able to see other members operations.

Chairman Crosby discussed an article written by one of our members Jess Stewart from Nevada Museum of Art. The article appeared in Security Management Magazine. He encouraged members with expertise in their field to write articles for the magazine.

Chairman Crosby announced that the May meeting would be held at the Washoe County Emergency Operations Control facility (EOC).

There was an open discussion of the following topics:

-We need members to RSVP for the monthly meetings so we know the number of meals to order. Charging members for the cost of a meal when they RSVP and don't show up was discussed.

The chapter needs to communicate better. Speakers and meeting locations will be announced earlier so that members can better plan on attending the meetings.

The chapter needs to work on increasing our membership. Members were encouraged to bring guest and recruit perspective members. We are making an effort to contact local and federal law enforcement agencies to increase their membership and attendance at meeting. Sparks PD has already committed to having SPD Officer Rodriquez become a member and attend our monthly meetings. SS Agent George Cheretis said he would assist in providing federal LOE contacts if needed.

We discussed getting better PR for the chapter by communicating with the local news agencies and possibly writing articles on security topics.

We discussed attempting to recruit business people as ASIS Members that may have broad responsibilities in their organizations that includes security.

Speaker
None Scheduled

Topic
Chapter Planning Discussion

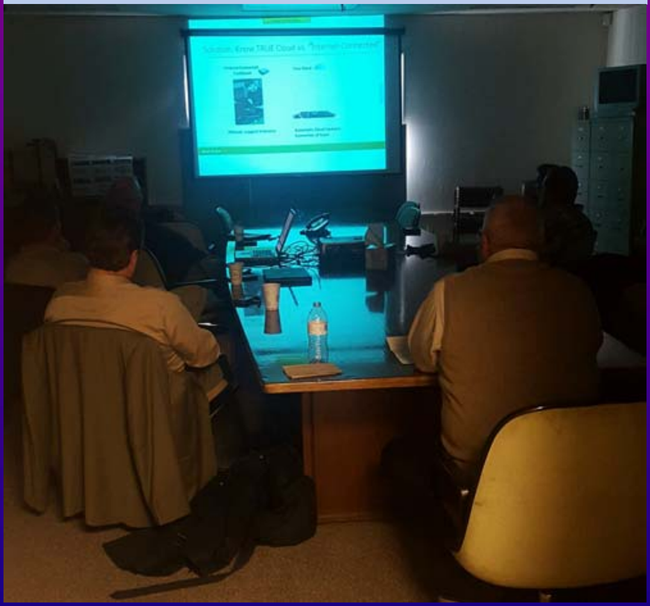
Next Meeting
Topic and Speaker to be announced

Drawing
A drawing was held for door prizes

Meeting Adjourned
1:18 PM

Michael S. Gach
Chapter Secretary

January 27th 2016
Webinar 1601-FUTUR: The Future Effects of Rapid Security Technology Change



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: UNR InNevation Center 450 Sinclair Street

Reno, Nevada 89501

(subject to change-check reader board)

Date: Wednesday, February 3rd, 2016

Time: 11:00 AM – 1:30 PM (approximately)

Thank you to Mike Pacini for bringing raffle gifts.

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	**Jason McLean**
Newsletter Editor	**Michael Smith**
Law Enforcement Liaison	**Dean Hill**
Legislative Rep	**Ken Braunstein**
Chapter Webmaster	**John Puccioni**
ASIS Foundation Rep	**Steve Foster**
Scholarship Chairman	**Ken Braunstein**
Chapter Photographer	**Ken Braunstein**
Audit Chair	**Ken Lightfoot**
Certification Rep	**Chris Brockway, CPP**
Young Professionals Liaison	**Steve Foster**

ASIS INTERNATIONAL
Advancing Security Worldwide®