ASIS INTERNATIONAL

YOUNG PROFESSIONALS

VOL II: Issue IV

2016 ASIS YP Council Chairperson:

Edward Batchelor

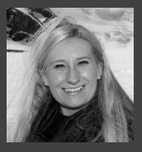
2016 ASIS YP Council Communication VPs:

Toby Heath

Elisa Mula

2017 ASIS YP Council Co-Chairs:

Angela Osborne



Michael Brzozowski

Commincations Team Lead

Zane Hickman

Newsletter Editor:

Ed Bloom

A MESSAGE FROM THE 2016 CHAIRPERSON, EDWARD BATCHELOR

As 2016 comes to a close, it's time to usher in new leadership to represent ASIS Young Professionals around the world. Over the last two years, I've had the privilege and honor to participate in this amazing organization as the Chair of the Council. Not only have we grown in all ways, but we're creating the future for the next generation of industry leadership. To continue on our uphill climb, Angela Osborne, PCI, and Michael Brzozowski, CPP, PSP will co-chair the Young Professionals Council in 2017. It's exciting and change can be good. Both Angela and Michael have poured their heart, sweat and tears into reshaping ASIS for the future. It was a pleasure serving as the first Chair of the Council and I look forward to supporting Angela, Michael and all young professionals in 2017.

A MESSAGE FROM THE 2017 CO-CHAIRS

A new year always brings change, 2017 is no different. We thank Ed Bachelor, Elisa Mula and Toby Heath for their dedication and efforts. The YP council welcomes new Co-Chairs Angela Osborne and Michael Brzozowski.

We think that we can all agree that 2016 has been an eventful year for professionals in security. As always, many of the events continued to prove the necessity for security practitioners that are capable of dealing with major threats and risks. Security professionals have been faced with airplane crashes, continued conflict in Syria and Iraq, the Rio Olympics, nuclear testing activities, high profile cyber incidents and active shooter incidents, to name a few. For the Young Professionals Council, we recognize that these events will continue to demand the need for qualified practitioners, and we remain focused on increasing our membership and deepening our commitment to career development.

We have re-committed ourselves to our mission of educating and developing young careerists by providing a forum to engage with security thought leaders, get involved with ASIS programs and activities, and connect with peers from across the globe. Our council is unique in that is not committed to one specialization or field. We are an open council that welcomes all ASIS International members. Our continued involvement in ASIS is essential to the survival of the society and the continued professionalization of security careers.

Our current leadership of Chairperson Ed Batchelor, PSP, and Vice Chairs Elisa Mula and Toby Heath, CPP, PSP has unified our organization, increased awareness of our activities, and been a voice for Young Professionals in ASIS and beyond. We are so honored to be taking on this great responsibility and know that we have big shoes to fill. We also look forward to Ed, Elisa, and Toby's continued guidance as Council Advisors.

As co-chairs, we will be taking on distinct roles. Angela will be liaising with the ASIS Headquarters, ensuring that we are in good standing with ASIS International and continuing to focus on ways to expand our career development efforts and opportunities for Young Professionals through partnership with ASIS Institutions and organizations. Michael will be focusing on expanding the YP reach around the globe, increasing our membership, and collaborating with other ASIS Councils. We look forward to working with our tremendous Council Members in 2017 and helping to grow this extraordinary group!

- Angela Osborne, PCI, and Michael Brzozowski, CPP, PSP

ASIS YOUNG PROFESSIONALS NYC CHAPTER CAREER FAIR - Jairo Borja

On November 14th, 2016 we held our first ASIS Young Professionals NYC Chapter Career Fair at John Jay College of Criminal Justice. With the assistance of John Jay College's Center for Career and Professional Development, we provided students and job seekers with an opportunity to network with various companies in the security field at all levels.

SOME OF THE PARTICIPATING COMPANIES:

G4S; Door Security Solutions of Metro-Upstate NY; Sentinel Consulting; Peace of Mind Technologies; UTI Global; Hanwha; Securitas ES; AMAG Technology, Inc.; MSA Security; Secure-IT; Corporate Security Resources; Aventura Security; Excel Security; Doyle Security Services; Dun & Bradstreet; Gleis Security Consulting; NYPD Intelligence Bureau; Securitas

1 Networking Opportunities – Whether it was John Jay College of Criminal Justice, Pace University, or Berkeley College, this was a great opportunity for Justice Studies, Cyber Security, and Security Management majors to get face time with various employers in their industry. It helped students better understand the many available positions in the security field as well as be proactive about their career path by allowing them to build a list of contacts on which they could call as they approach graduation.

2 Transition Assistance – From law enforcement to military, we wanted to ensure that transitioning professionals had the opportunity learn about potential positions and their qualifications. This provided an opportunity for our security professionals that do not have private security experience a chance to gain exposure to the types of qualifications and job-specific expertise that a company like Aventura or Securitas may require. Whether it is in formal education or self-directed curriculum, it was an important reminder that differentiating oneself from other candidates can make all of the difference. Always remember to ask, "What makes me stand out more than others?"

3 Kickstart Job Search – The Career Fair also presented a unique opportunity to be face to face with the NYPD Intelligence Bureau and Dun & Bradstreet. It was a great opportunity for self-promotion prospective employers. Especially if it is an organization that you have been trying to interview for. It is important to remember that a resume only gets the interview, and behavior and good impressions are what land the job.

4 Elevator Pitch Practice – Even if students and job seekers were not completely sure of their position interest, the Career Fair gave attendees chances to tune their elevator pitch.

5 Human Touch – Applying online only provides so much exposure. By attending the Career Fair, we provided an opportunity to make contacts with organizations beyond recruiters. Rather than having to deal with this added layer, attendees were able to build a personal connection with prospective supervisors.

In conclusion, we would like to thank Demerle Lewis and Dov Horwitz for bringing the idea forward and executing. Timing could not have been better with ISC East following a few days later. The Career Fair successfully provided the opportunity for students and Young Professionals direct exposure with the organizations that are recruiting for entry level to senior level positions. Even if an attendee did not make their ideal contact, they at least had the chance to visit with professionals that are currently shaping the industry. It is always important to stay ahead and learn what soft wares or skills are needed to stay ahead in the security field.

ASIS YOUNG PROFESSIONAL ON THE MOVE - Scott Young

Scott Young, Senior Director of Business Development at GardaWorld, recently graduated from Athabasca University's MBA program.

Scott started the program January of 2013 The program was demanding, occupying 15 hours per week of his time on top of his work responsibilities at GardaWorld, who Scott said could not have been more supportive, and that this achievement would not have been possible without their support.

"Acquiring this degree, I've been able to better understand the Security industry in Canada and apply contemporary management best practices to our operations."

http://business.athabascau.ca/mba/online-executive-mba/

YOUNG PROFESSIONALS

A MESSAGE FROM MICHAEL BRZOZOWSKI: 2017 CO-CHAIR

In my current role as the Risk & Compliance Manager for Symcor, one of Canada's largest financial processing companies, I am responsible for the design, implementation, management, and maintenance of Symcor's physical security systems, as well as the development and maintenance of Symcor's governance and compliance programs. I earned the PSP and CPP certifications, as well as the basic and advanced Crime Prevention Through Environmental Design certification. These accomplishments have resulted in a very satisfying career and the very humbling experience of being named to the Security System News "Top 20 Under 40" class in 2016.

I became a member of ASIS in 2009, and I am proud to have been part of the ASIS Young Professionals program since 2012. Initially, I started out as the co-chair of the Young Professionals committee in Toronto, and as a result of the successes of the Young Professionals activities in Toronto, I was invited to join the ASIS International Young Professionals working group. That working group has since evolved into this very council, and since 2013, I have held various positions within the council including secretary in 2014, heading the YP Global Outreach efforts in 2015, and finally having the opportunity to be a co-chair with Angela in 2017.

I am thrilled to be working with Angela and the other Council Members in continuing the momentum that was built by Bryn, Elisa, Ed, and Toby over the last five years.

A MESSAGE FROM ANGELA OSBORNE: 2017 CO-CHAIR

We cannot say for certain what 2017 holds, but Michael and I are committed to strengthening the Young Professionals Council.

For some background, I am the Regional Director for Security and Technology Consulting for Guidepost Solutions in Washington, DC. Prior to that I worked for Interos Solutions as a Senior Analyst for our clients at the Office of Cyber Security at the US Department of Commerce, NASA Goddard Space Flight Center, and GSA. I spent several years in the Middle East working for an energy company, performing risk assessments on power plants and well sites.

While my home chapter is the National Capital Chapter, I helped to found the Abu Dhabi Chapter of ASIS. In 2014, I was selected as a Seminar Experience Recipient and joined the Young Professionals Council. This year, I worked closely with our Council Members to put on the Young Professionals' Career Center at the Annual Seminar in Orlando. In the coming year, I plan to find more ways to make ASIS education and events more accessible for YPs around the globe.

DENVER - PIKES PEAK NETWORKING EVENT

The Denver Mile-Hi and Pikes Peak Chapters in Colorado jointly hosted a first-class networking event for Women in Security and Young Professionals. Nearly 100 attendees took part, including dozens of students and young professionals. The Group 1 Senior Regional Vice President Jeff Slotnick, CPP PSP, spoke on the benefits of ASIS membership, while Michael Petty, the Regional VP 1E highlighted the ASIS mentoring programs. Bryn Palena, the founder of the Young Professionals Council also attended and talked about how the council helps develop and grow the careers of young professionals in the security industry.

"Just under a hundred attendees enjoyed networking at the YP/WIS event, which was co-hosted by the Denver & Pike's Peak Chapters."

The event included hors d'oeuvres and beverages in a beautiful setting in the foothills of the Rocky Mountains. In addition to the great networking opportunities, there were several door prizes, including gift cards as well as 6 people selected for free professional photos. A special thanks goes out to the sponsors as well as chapter board members who all worked to make this event possible.

YOUNG PROFESSIONALS

FIVE TECHNICAL MEASURES TO SECURE PHYSICAL INFRASTRUCTURE

W. Jackson Schultz, CISA is a Senior IT Audit & Security Consultant at OCD Tech where he is responsible for increasing business growth for the OCD Tech division, as well as holding both an outsourced CISO and IT audit role for a variety of the firm's customers. Additionally, in October, he will begin his candidacy for the Brown University Executive Master in Cybersecurity.

The impending bridge between our technical and tangible worlds has generated lively discussion among physical and cyber security industries. Any executive forum or conference agenda today related to our industry includes conversation surrounding the Internet of Things (IoT). Professionals on both sides have anticipated this amalgamation for years, and now that it has finally arrived, we must take proactive measures to secure infrastructure from numerous threats. We must execute this in the background, while ensuring that employees, business associates, and customers have a strong user experience. Listed below are five technical controls which, when implemented, will assist in securing physical environments.

1. Access cards – implementing a system that provides access to users through the practice of unique identifiers, such as utilizing radio-frequency identification (RFID) cards, is a strong technical security control that will ensure accountability. Each time a card is swiped, a one-off number is linked to the card of the user, whose access can be monitored to see what specific locations they visited. The second key element of this control, however, is to perform a periodic access review (scheduled as often as is determined by a risk assessment). Failure to review user access to a sensitive area almost entirely negates this control, and generally yields the same result as using a lock and key.

continued on page 5

ASIS FOUNDATION: HIGHLIGHTS

The ASIS Foundation is focused on three things: investing in our members, supporting research and enabling projects that benefit our communities. In 2016 we accomplished a lot in all three areas! We published a very well received CRISP report focused on sports team travel security that we made even more accessible to our members worldwide through a newly launched microsite. We helped over 150 people around the world pursue education and career development with scholarships and awards worth over $440,000. And the Foundation supported ASIS councils, chapters and members in donating $45,000 to local communities and military veterans.

Alan J. Cross Award
20 on-line certification review courses available on a first -submitted, first-awarded basis.
Apply January 2

Chapter Matching Scholarships
Awarded annually to students and members pursuing degrees in the security field. This special scholarship combines support from the Foundation with chapter support.
Apply January 2 - November 20

University of Phoenix Scholarship
Five full tuition scholarships for security professionals pursuing an undergraduate or graduate degree.
Apply February 1 - March 29

Webster University Scholarships
Two full tuition scholarships to ASIS membersto pursue graduate degrees in business andorganizational security management.
Apply March 1 - May 5

TAHC Certification Scholarship
Pays for application, exam fees, reference set and on-line review course for ASIS members working in law enforcement.
Apply May 8 - July 3

MLC Certification Scholarship
Pays for application and exam fees, reference set and on-line review course for ASIS active duty military.
Apply May 8 - July 3

Timothy J. Walsh APC 1 Award
Provides tuition, travel and hotel for one member to attend APC I.
Apply May 9 - July 1

Chapter Awards
LELC Public Private Partnership Award
Provides full travel stipends for 2 public private partnership program heads to attendAwards Presentation at Seminar.
Apply April 24 - July 3

Roy Bordes Physical Security Award
Provides a two-day physical security program based on chapter needs.
Apply October 20 - December 16

FIVE TECHNICAL MEASURES TO SECURE PHYSICAL INFRASTRUCTURE - CONTINUED FROM PAGE 3

2. Multifactor authentication (MFA) – single factor authentication, such as a password or an identification card, is no longer a strong enough control to protect unauthorized access to sensitive areas or data. Hackers are using such advanced techniques that they are bypassing these systems at a very fast pace. Implementing a second form of authentication to work in conjunction with the first is now more important than ever. The goal of multifactor authentication is to ensure an individual is who they claim to be by requiring two or more of the following attributes: something that you know, something that you have, and something that you are. Something that you know could be defined as a password or a personal identification number (PIN). Something that you have would be an identification card or a badge with a chip. Finally, something that you are is generally biometrical: a fingerprint or scan of a retina. Multifactor authentication provides strong assurance that only appropriate individuals are granted access.

3. Networked security devices – the benefits of security devices such as security cameras or motion sensors are well-recognized within both the physical and cyber security industries. Monitoring and alerting about inappropriate access is an effective detective process that identifies potentially malicious behavior. One procedure that many system owners forget, however, is to change the default credentials of installed networked technologies. Many of these devices are internet-facing and can be accessed over the web. The problem with this is that if default credentials (either for general or administrative access) are not changed, malicious users could browse and log into the devices' IP addresses as easily as a Google search for these manufacturer-issued credentials. From there, this individual could watch footage or live stream through the cameras, disable them, or edit and delete footage. Consequently, these devices have then become more of a liability than an asset. Additionally, the distributed denial of service (DDoS) attack on the domain name servers (DNS) hosted by DYN a few weeks ago happened because there was a botnet network (zombie computers controlled by a remote attacker) accessing these Internet of Things (IoT) devices through unchanged default credentials, in some cases similar to security cameras and motion sensors.

4. Security awareness training – while this is not explicitly a technical control, it is still a valuable measure to implement within various organizations. Many times, cyber security professionals find security awareness training to be synonymous with emerging threats information sharing and phishing testing. These are both elements of this training, but as the Internet of Things (IoT) continues to gain acceptance, other measures must be added to the training. An example of this is familiarizing employees with other methods of social engineering, such as tailgating, vishing, and impersonation. Each of these threats can negatively impact an organization as much as an employee clicking on a malicious link. Additionally, there are technical devices that a threat actor, or individual with criminal intentions, may use to compromise a network, such as a LAN Turtle, Raspberry Pi, or Rubber Ducky Deluxe. Physical security professionals should become familiar with these devices, their purposes, and how to identify them.

5. Termination procedures – the insider threat is a topic that garnishes a lot of attention because of the damage that an employee can do to an organization. Many times, a disgruntled employee either leaving an organization or preparing for termination will act inappropriately with the permissions they have been provisioned. Ensuring strong termination procedures are in place is critical to the protection of information. Two-weeks notice used to be the norm for transitional reasons, but with advancements in technology the need for this, in most cases, no longer exists. Physical security professionals should be trained in termination procedures and to anticipate scenarios related to the insider threat, as well as in tactics to stop sensitive data exfiltration.

These five methods are not a silver bullet to protect an organization 100% of the time, but practicing strong controls, policies, and procedures can drastically decrease the time an attacker will spend trying to compromise a business. For more information, please visit www.ocd-tech.com to learn more ways that technical advancements can assist physical security professionals.

WE WANT YOU TO PARTICIPATE

Thank you for reading the latest version of the ASIS YP newsletter. Our newsletter is distributed quarterly and highlights Young Professionals from across the country. The key to the newsletter is the support and content from you the reader. Please send any YP related events or articles to ASISYoungProfessionals@gmail.com. We look forward to receiving your contributions as we work together to share the achievements and successes of Young Professionals around the world.

- Zane Hickman,
ASIS YP Communications VP