Direct from an ASIS INTERNATIONAL COUNCIL

White Paper
ASIS Council Security Services and Women In Security

HOW TO PLANT THE SEEDS TO SUCCESS IN THE SECURITY INDUSTRY

By: Sandi Davis, Lisa Dolan, CPP, Lawrence J. Fennelly, CPOI, CSSI, Karen A. Frank,
Robert P. Giordano, Dawn Gregory, CPP, Susan E. Hunter, Marianna Perry, M.S., CPP,
Gail Reece, Laurie Simmons, CPP, PSP, Lina Tsakiris, CPP

Purpose

This white paper has been prepared for ASIS International by two of its councils: The Security Services Council and the Women in Security Council. This white paper seeks to outline these significant developments and others in the security industry and to foster further discussion, analysis and solutions. Certain materials from which this white paper is derived emanates from an online survey the two Councils created, consisting of 27 questions, answered by more than 200 participants. There are several that contributed to this work thus, some of the contents may overlap, allowing for a stronger punctuation of the concepts and themes introduced.

Women In Security Council:

The Women in Security Council (WIS) provide support and guidance to women in the security field, as well as inspire those interested in entering the profession. While this group's benefits and programs are tailored for women, we encourage and welcome the participation of all members who are dedicated to the support of women in the security industry.

WIS offers a monthly forum where industry leaders discuss relevant topics such as breaking barriers and effective leadership. The intimate group setting yields open and candid discussions among participants as the hosts share their experiences in the industry.

Acquire new knowledge and strategies relevant to your personal career goals through our specialty programming. Accomplished professionals share their unique expertise and insights into issues challenging women today, training and education as well as leadership in all aspects. The Council promotes and supports the goals and objectives of ASIS. It consists of a volunteer base of highly respected and educated women and men in the industry. The contributors of this White Paper are recognized leaders in the security industry and are at the pulse of what is occurring in our industry.

Security Services Council:

The Security Services Council, the leading resource for education, outreach and suggested practices for all the industry's manifestations, including officers, alarm monitoring, investigations, security design and implementation and other contracted services in support of a security program. The Council conducts educational workshops and webinars, participates in industry associations and partnerships, and promulgates industry best practices.

Introduction

Galloping across the western plains on a mighty steed, the man sports a bushy mustache, a wide-brimmed hat, armed with a six-shooter gun and rifle. This is the image from Americana, circa 1850; enter America's first security professional, the Pinkerton detective.

The image is now considered anachronistic, historical even. So much has changed since then, the "Industry" developed, evolved and is now integral to the successes of global security. Security is now considered a professionalized, worldwide industry with thousands of disciplines and specialties utilizing the latest in technology. What traditionally was also considered a male only occupation now sees a steady inclusion and growth of women in the industry. Certifications through accredited organizations such as ASIS International and the International Foundation for Protection Officers (IFPO) along with college courses – like those through the IFPO's recent partnership with Kaplan University, ensures that security professionals are more qualified than ever before.

Certainly, the need for competent security practices has become paramount since the Pinkerton detective. The nature of technology based security threats require an entirely different skill set than traditional physical security roles. These changes have resulted in an industry shift whereby law enforcement or military experience is no longer viewed as prerequisites for employment in the security industry (*According to the SSC/WIS Survey 2017). Thus, careers in the field are now pursued by young women and men whom possess educational requirements that directly align to the role. This is a strong departure from police or military personnel that enter the private sector as a second career engagement. Many of these young individuals are earning four year college degrees to advance their careers.

Statistics bolster the anecdotal evidence: "Security is one of the fastest-growing industries", according to the U.S. Department of Labor*[1]. At the vanguard of the industry is ASIS International (ASIS), leading professional security organization based in Alexandria, VA. ASIS boasts 242 chapters across the globe with members from both the public and private sectors, from entry-level officers to top security industry executives. ASIS works with members to lead the development of important industry standards and offers important networking and various volunteer leadership opportunities whereby enterprising individuals can really embed themselves in the industry. Each year, ASIS holds their annual seminar and exhibit in a major city. ASIS also holds an annual European counterpart seminar to the United States' event.

The stereotype of the inept rent-a-cop is often part of American pop culture. Look no further than Kevin James, the lovable, blundering Paul Blart "Mall Cop" character. The negative portrayal may appear insurmountable, yet the perception continues to be defeated due to the demands caused by municipal financial burdens and the increased need to augment public security requirements with that of private security officers. This may very well be the modern iteration of the law enforcement officer and is strongly reflective of where the industry is headed overall. A recent story by Albuquerque, New Mexico station KRQE reports that a city council member suggested the hiring of security officers in an effort to rein in police overtime costs, counter its police officer shortage and combat the increase in downtown crime.

The Evolving World of Security

The security industry has traditionally been male dominated with a heavy proportion of former law enforcement and military personnel. According to a September 2016 study by ASIS International and prepared by McKinley Advisors, 25% of security professionals have a law enforcement background and 24% have military experience. It is also not surprising to note that 87% of security professionals responding to the McKinely Advisors survey were men.

Although men vastly outnumber women in the security field, as the demand for qualified security professionals continues to grow there will be a significant number of high-profile positions available for both men and women.[1] Regardless of gender, knowledge of current trends and issues remains a critical component in the professional development of all security professionals; especially those hoping to reach the highest levels in the industry. Those who truly hope to make the most of their professional development can gain significant credibility by earning the certifications offered by organizations like ASIS International or the IFPO, perhaps in addition to formal educational degree programs. This rise in training opportunities, involving significant amounts of industry-specific knowledge, will give security professionals more flexibility in achieving career goals; and increased respect in the corporate boardrooms that many high-level security leaders find themselves needing to navigate.

Current Trends: How We Arrived Where We Are Today

Is it possible today to enter the security profession without having any law enforcement or military background experience? It absolutely is.

It is well established that a large majority of older generation security professionals came to their roles from a law enforcement or military service background. Even today, most college criminal justice programs are geared to the law enforcement professional and are slow to adapt to addressing the security profession. Roughly one-third (36.22%) of those surveyed for this white paper felt that a law enforcement career or military service adequately prepared them for a security professional career in the private/corporate or government sector; whereas another one-third (35.20%) replied no that they felt that the law enforcement/military career had not played any role in their career path. The remaining slightly less than one-third (28.57%) had no opinion on the effects of the prior experiences.

Today's security industry boasts diverse paths to industry employment for non-law enforcement or non-military individuals. It appears that the former assumption of required law enforcement or military experience is being challenged by the changing needs of the industry and the diverse skill sets of those entering the industry.

Of the 205 individuals who responded to our survey, 56% were women and 44% men. A surprising 71% of respondents had no prior law enforcement background, compared to 29% who had entered the industry with law enforcement experience. Similarly, 22% of respondents indicated a military background, compared to 78% who entered the industry without prior military service. If our survey results are indicative of a larger shift in the industry, many of today's security professionals have not come from some sort of law enforcement or military services. Rather, they have presumably brought a breadth of different experience to their role to make the security industry what it is today.

The survey also sought to understand under what circumstances were respondents' first exposure to the industry. A combined roughly 20% indicated it was through law enforcement or military, while half of participants (50%) indicated that it was "on the job". There was a 50/50 split in respondents as to whether they intended to become employed in the security industry, or whether the industry "found them", for lack of better words.

Paradigm Shifts That Are Changing Our Industry

Definition of a paradigm shift:

> A paradigm shift, as identified by American physicist Thomas Kuhn, is a fundamental change in the basic concepts and experimental practices of a scientific discipline.
>
> websitehttp://www.theinfolist.com/php/HTMLGet.php?FindGo=Thomas_S._Kuhn

Look at where the security industry was 20 years ago and then take a look as it is today. Several paradigm shifts have occurred as indicated in the results of the SSC/WIS Council 2017 survey.

The most notable paradigm shift is the increase in security professionals who did not enter the industry with a law enforcement background. We are seeing a great deal more security professionals coming from non-traditional backgrounds including business administration and social sciences. Non-traditional backgrounds bring a different and enhancing perspective to the industry, offering a variance in perspective and problem solving. This diversity challenges the formerly myopic approach to security, when most professionals came from a law enforcement or military background. The diversity offered by security professionals who come from non-traditional areas such as retail, human resources and business management, give the industry a different set of values and practices which are considered a break away from former approaches to security.

However, a question still begs answering. Is this a positive paradigm shift? The answer can only be known if the outcome of these shifts is that we become collectively safer and smarter. Like a tectonic shift, each new change wrenches us from our established paradigm and forces us to reflect on our current approach. Are our approaches and procedures intentional or habit?

Change and diversity in background will have positive impacts on the security industry. We must not leave behind the knowledge and experience of law enforcement backgrounds, but we must also be accepting of other diverse backgrounds and what they can offer to our industry moving forward. In fact, former law enforcement professionals transitioning into the industry may not be adequately prepared for the much more complicated and multifaceted industry they find themselves in and the tool set of a law enforcement officer may require augmentation. For example, much of law enforcement work has evolved through the reactive mindset. Bad people do bad things and law enforcement responds. There is nothing inherently wrong with this approach and it usually serves law enforcement and emergency response personnel very well. The security mindset often requires a proactive, if not predictive approach in order to effect prevention and mitigation. Corporate security managers and directors require a big picture approach to enable proportional risk treatment and employee protection strategies. This is the basis for Enterprise Security Risk Management (ESRM) which is a key essential skill for security practitioners. The security practitioner must develop a preventative mindset and expand their skill set through achievement of professional certifications like the Certified Protection Professional (CPP) certification, the Physical Security Professional (PSP) certification and the Professional Certified Investigator (PCI) certification offered by ASIS. There are several others categorized by field, the CISSP, Certified Information Systems Security Professional for Cyber Security, the CEM, Certified Emergency Manager, the Certified Protection Officer (CPO) and Certified in Security Supervision and Management (CSSM) offered by the International Foundation for Protection Officers (IFPO). A certification, like education, is the great equalizer. Certifications in these disciplines demonstrate the essential commitment and tested experience that states loudly that you are knowledgeable in your field. There are also many more educational opportunities today than a decade ago. Degrees in Homeland Security, Cyber Security, High Rise Security, Executive & Dignitary Protection and Conflict Resolution are increasingly available through reputable learning institutions. The possibilities are vast and available both on line and through traditional in person learning. Roughly 21% of survey responders mentioned before have a CPP designation and 44% have a bachelor's degree. Of those with bachelor's degrees, only 11 of 175 respondents are in Security Management roles. The trend to obtain certification and/or degrees in security specifically is on a strong uptick, however there is still much more room to expand in both fields.

Predicting The Future

Predicting future security threats with 100% accuracy still remain a challenge for a business, although notable progress through Advanced Intelligence (AI) is being made. Making reasonably effective projections based on thorough analysis and forward thinking so that potential problems do not become actualized.

The trend we are seeing now is an uptick in the proactive mindset and methodology being embraced. Proactive approaches to security have become more than fortifying windows and identifying potential access points. As the threats facing us today grow more sophisticated, the security professional must be devoted to proactive measures designed to deter in order to keep the business operational.

The consequence to not being proactive can be critical. There are too many examples and the detrimental impacts of reactionary security response. One that comes to mind is the bullet proof windows being placed in some squad cars. This was a reactive implementation based on several officers being ambushed while in their patrol cars. If we look at the implementation of body cameras we can trace that back to the incident in Ferguson. The reactive approach to security focuses on responding to past and present threats vs anticipating future problems/dangers before the symptoms manifest. Absent a critical incident, the implementation of body cameras for law enforcement may not have been accepted. It was due to the questions surrounding the circumstances of the shooting that opened the door to the discussion of body cameras. Do you remember the shoe bomber? The implementation by the aviation security industry of the extreme and sometimes ridiculous screening by having to remove your shoes is a prime example of reactive methodologies implemented at each airport. Making long term strategic decisions and assessing strengths and weaknesses and opportunities and threats are all important components of the proactive vs reactive mindset.

People

There are several notable shifts in the people aspect of security, all of which have greatly shaped the idea that a career in private security is a real and viable consideration. This involves not only choosing to be employed in the private security sector, it's also about creating a career that matters by mindfully applying a career road map. There is much contemplation today about applying awareness to our lives and our careers. There has been a strong shift from the "falling into security" mentality to one of "choosing and constructively pursuing" security as an enduring career choice. The pathways in security are varied and can afford unique avenues into many exciting areas. There is great opportunity for uniqueness for today's security professional in building their own "brand" of skills specialization and understanding that the path to success has many roads to choose from.

Process

Perhaps one of the most material shifts in the private security sector in terms of how we "do" security is the reliance that the public sector now has on private security offerings. This reliance has increased the value of private security, driving the marketability of private security professionals. This may be less of a phenomenon in Europe, Africa and the Middle East where for decades, we have witnessed private security serving in operational and strategic roles. We also see today an increased need for intelligence and analysis information exchange from private sector to law enforcement and other government agencies (the public sector). It is the private security official who will often notice suspicious activity or know when something is simply out of place in the environment that they protect. Having this type of increased awareness at the "streets and sidewalks" level is a force multiplier for government agencies that are often not funded to offer an adequate span of coverage. The security professional is, in many cases, the real first responder to a scene. Often trained in observing and reporting, this individual is expected to respond to emergencies such as medicals, evacuations and incidents. The security professional will be the safety professional that will observe and note safety hazards and violations. The security professional will be the emergency management professional that will observe and reports risks, offer mitigation strategies and provide preparedness training. The importance of security's role as first responders cannot be overstated. Having as many trained eyes and ears observing and reporting in society today is critical for protecting employees and businesses.

The funding and capability of large global corporations operating in high risk environments or attractive sectors such as banking, energy and nuclear, are investing in building their own fit-for-purpose intelligence departments to stay at the forefront of security risks. Intelligence gathered by these departments may now be readily shared in an actionable format with the public security sector through established and formalized conduits. This not only alleviates the idea of segmentation but spotlights the importance of the collaboration needed between the two sectors to ensure we remain effective in our overall approach to mitigating ever increasing and sophisticated threats.

Today, corporate security is typically represented at senior executive levels within the organizational structure and is a key driver to the success of the organization's overall mandate. We have moved well beyond the traditional focus of locks, key and guards to a place where intelligence-based security programs staffed by highly educated professionals are essential. The roles of CSO and CISO exist to ensure that the responsibility and authority to make appropriate risk-based decisions happens at the highest level and encapsulates the idea that security underpins all aspects of the organization; from operational security that protects physical assets to strategic approaches that are aimed at protecting against sophisticated and complex cyber attacks.

Today's security professional has myriad opportunities to explore an enduring and worthy career in the private sector. The key to their success will be their ability to build an arsenal of deep technical skills while ensuring they also have capability in the business environment and are equipped with the acumen to convey the value of security to their organization in a way that is consumable to non-security executives. Contributing to this arsenal is the ability to mentor and be mentored. The Security Services Council and Women in Security Council Survey Results- August 9, 2017, notes that since joining the security industry, 28.43% of survey responders had a mix of both male and female mentors. Mentoring is extremely important and the benefits are concrete and long lasting. While we still find that the majority of mentors in this industry are male, 32.99% in comparison to just 7.61% that were female, any mentor-ship is a great thing. Mentors are a guide and sounding board and can help navigate through the industry as a whole or focus on a specific goal such as obtaining a Certification.

Technology And Infrastructure

Security and associated protective technologies are always in a state of evolution. The induction of security technologies aimed at detection and deterrence of adversarial activity in the private sector are commonplace. The significant change in today's security technology is a shift from technology as a support resource to survey and alert to when bad things are happening, to technology as a tool to automate traditional security functions and even predict where and when bad things could happen. This shift brings us to recognizing "the art of the possible" in that security is no longer reactive and has become intelligent in managing today's threats.

Success for today's security professionals will require competency in both physical and logical security domains. The idea of convergence in these two areas has moved from a once contemplated phenomenon to a strong reality. Organizations that operate in the private sector are showing the value of convergence by integrating the capabilities of their physical and logical security teams to ensure they have a 360-degree view of risk.

This holistic approach to asset protection drives effective and efficient protection models while matching and hopefully exceeding the sophistication and capabilities of criminal networks that are highly motivated. In addition, great investments are being made in automation to ensure the speed of detection and response to vulnerabilities is at the forefront of the corporate security program. The impact of automation is significant to the security professional, as many of the traditional roles that were once served by a security guard are now replaced by technology that is supported by a new type of security personnel. This new security professional will need to be adept at understanding how to leverage technology, to ensure a best success outcome.

The success of the security professional will continue to be shaped by the evolving threat landscape and by organizational needs. Remaining marketable by investing in appropriate education and ongoing participation in security associations is critical. Today's security professional must be diverse and understand big picture strategy to positively impact organizational needs by finding solutions that enable business objectives while mitigating threats in and outside of the organization long before they materialize.

To see where the industry is going, we should take a closer look at who made up the respondents of the SSC/WIS survey. The responses indicated that 71% were not currently nor had they been in Law Enforcement; 78% have not been or were currently serving in the military; and 73% did not believe having a law enforcement or military career background are critical in having a successful career in the security industry. 44% of the respondents have a Bachelor's degree with 35% having the degree in Criminal Justice, 33% in Business Administration, 19% in miscellaneous discipline, 11% in Security Management, 10% in Psychology. The age of the respondents varied in age from 18 to 75+ with 21% between 25 and 34, 32% between 35 and 44, 25% between 45 and 54, and 15% between 55 and 64 which shows the known three generations active in the overall workforce. 56% of the survey respondents were female and 44% were male.

Where will security be in the future and what will it take to be successful in the industry? Today, security technology is fully integrated through alarm monitoring, access control, video surveillance, identity management, RFID, HVAC, robotic patrols, communications, automated bollards, bio-scanners, shared database, and the platforms that bring all these together. We know that having a "better than basic" understanding of technology is critical.

But, what else will security professional have to battle? Economic Information Warfare (EIW) against economies, commerce and enterprises will continue to escalate as a global threat. Smart watches, a new generation of super-sensitive satellite and video network electronic surveillance will be everywhere. Real-time personal face scanning and identification, sniffers designed to automatically sense, watch, and search for specific people and things, and massive computing power will continue to serve both (good intended) security entities and malevolent threat actors. Weapons will have the capability to navigate physical, wireless and electronic countermeasures. Identity cards with embedded smart chips containing a person's entire genomic profile will be used to authenticate wirelessly and remotely. The use of embedded nano-chips will allow for GPS tracking. Embedded biometric authentication and security tattoos with bar-scans may become popular and fashionable. Digitally Engineered Personalities will be integrated into the global telecom networks and provide full time tracking of individuals, enterprises and governments. The continuing proliferation of self-mutating computer malware created to destabilize, confuse, and collapse critical infrastructures will grow globally. Bio-war and agri-terrorism will become common threats against public health, food and water resources.

Individual privacy "violations" will continue to grow and the legal system will be challenged with balancing personal freedoms with security. *[2]

What does this mean for the security professional? For those in the military, there are several avenues that will train men and women to combat the current and future trends.

We have seen the rise of non-traditional security careers through TV and movies including NCIS and Criminal Minds; these programs are military and law enforcement based, but they have increased the popularity of this type of work in the private sector. Additionally, the casts present a wide range of diversity.

The video game and robotics industries are unlikely influencers on the security industry. Battlebots and drone technologies are blazing the trail for new avenues in security. Robots with learning capabilities are being used for security patrols. Drones are being used in commercial security applications, which require specific pilot's licenses. Drawing the line from drone racer to drone security provider offers an indirect career path to enterprising young individuals interested in joining the industry.

As the age of our industry leaders decreases, all of this will play a role in how our industry moves forward. According to Manpower Group, by 2020 Millennials will make up 35% of the global workforce. They have never known a time without technology. Many will rise to leadership roles where they may supervise Gen-Xers and even Baby Boomers. Being in the "boss chair" and managing a workforce older than them could be a strange experience. This will change as the older workforce retire. In the meantime, there are hurdles to watch. Millennials are the emerging leaders. In particular, women are changing the way leaders address their co-workers. Many go out of their way to let them know they are respected, heard and reinforce that each person is an expert in their field. Our younger leaders are learning why their managers were impatient; at the end of the day, you pick your battles and everyone relies on your vision. Having people around you with decades of experience can be one of those battles. Meanwhile, Gen-Zers are entering the workforce. They tend to be more efficient and productive because they are used to managing several things at one time. Gen-Zers saw their parents lose a lot and have learned to work for what they want. More young people do not want to stay with a company, they would rather start their own business and consult. Millennials believe in going after certifications in their field and they want their organizations to pay for them. They also want more than money; they want to believe that what they are doing has meaning on a bigger scale. And they need to see that greater cause. *[3] It is interesting to note that in the SSC/WIS survey, 68% of respondents noted they had no industry certifications. According to the survey results, 69% are looking for skill development in leadership/management, 58% in security (asset protection, travel security), 50% in investigations and intelligence, 37% in information technology (computer forensics), and 34% in business acumen; it should be noted that this was an open-ended question. One thing is for sure, security professionals are looking to expand their skills.

Another challenge with the changing landscape of business, in general, is the notion that people can work from anywhere and should be provided the tools to do so. This supports Millennials wanting to contract instead of staying with companies. It has given rise to "co-working spaces" in many cities. It allows for remote work while maintaining face-to-face connections. Younger workforces are attracted to the flexibility and stability that a hybrid working model brings. This may also result in retaining talented individuals. ~~(3)~~ *[4]The results of the SSC/WIS survey demonstrated that 37% of respondents felt that communication is the most important skill set to be successful in a long-term security career.

The hybrid of remote/in-person work space will have an impact on improving this skill.

Being able to adjust to the changing threat landscape, stages and actors is going to take agility, progressive thinking and action. What worked yesterday may or may not work tomorrow. As we have seen, the career path to security leadership is beginning to change and will continue to do so. The old saying goes, "The only constant is change." Being highly specialized in one or two areas of security, with a firm understanding of how other areas integrate with each other will be critical. Degrees and life experience will be a starting point with specialized certifications helping to fill information gaps in the security practitioner's tool belt, and an important competitive differentiator from one candidate over another. Being able to reinvent oneself and apply transferable skills multiple times through their career to adapt as things change will be become the norm instead of the exception. A higher rate of cooperation and interoperability between disciplines and the ability to utilize agile development and problem solving will be necessary for a more complete Enterprise Security Risk Management. Developing and fine-tuning interpersonal skills will continue to play a key role in succeeding in the security industry. Success will depend on being able to effectively communicate across multiple levels and industries in order to convey a message.

The face of the security professional is changing and will continue to do so. The proliferation of technology is changing the threats to businesses and governments; how we do business; and how we, as security professionals, will need to protect what we are responsible for. The education and career path of a security professional will likely not be consistent or traditional. Once in the industry, the path a professional chooses to adjust to the changing landscape is what is going to be important.

Sometimes when we as security professionals discuss the future of the security industry and attempt to identify emerging trends, it's a bit difficult because there are so many different areas to our discipline. For example, when the book, ***Security in the Year 2000***, was published by ASIS International, computers were not mentioned. **The book, *Security in 2025*** is now available and much of that book is devoted to technology in the security industry.

One of the latest innovations in the security industry is the use of robots to perform security tasks. Robots built in the Silicon Valley by Knightscope, are available to Allied Universal Security clients nationwide, and these Autonomous Data Machines (ADMs) have the ability to scan for and detect issues that could lead to threats, in addition to analyzing anomalies and notifying the security team. These robots will perform real-time patrols utilizing the K5 (outdoor) and K3 (indoor) models. Highlights of some of their features, include:

- **360-degree video** that provides complete awareness and feeds to a security operations center.
- **Thermal imaging** for identifying fires and gauging proper environmental temperature settings.
- **License plate recognition**, which is an example of a computational task that may include data collection in a large parking facility.
- **Intercom and broadcast capability** that can be programmed to relay messages or alert security personnel to immediately dispatch law enforcement.[1]

"As our clients' needs evolve in the security realm, so must our solutions," said Dennis Crowley, Allied Universal's Vice President of Technology. "Smart robotic technology is the next evolution in security, therefore, our goal is to introduce it to as many customers as possible to give them another viable option."[2]

Robots performing duties that were previously the work of security officers are examples of the new technology available in the security industry. The well-educated security professional of the 21st Century has already grown accustomed, by necessity, to advanced technology to stay abreast of changing trends, and the following is a list of projected trends:

Summary

Fifty Emerging Trends In Security From The Past Five Years To The Future:

1. IT Infrastructure Protection Planning
2. IT Infrastructure as a Single Strategic Plan
3. Infrastructure and CPTED partnership
4. Mitigation Strategies
5. IP and Digital Video
6. IP Security Provisions
7. Security IP Edge Devices
8. HD Cameras and Monitors
9. Video Analytics
10. Visible Light Cameras
11. Thermal Imaging and Cameras
12. Thermal Imaging Sensors
13. Perimeter Protection
14. Layers of Protection Analysis (LOPA)
15. Visitor Management Systems
16. Mass Notification
17. Active Shooter/Active Assailants
18. Cloud Storage and Computing for Security
19. Advancement of CPTED Concepts
20. Contractor Pre-qualification
21. Emergency Management & Planning for Disasters
22. Software for Physical Security Maintenance
23. Laser Communication
24. Drones: A Safety and a Privacy Issue
25. Encryption
26. Critical Thinking
27. Soft Targets v. Target Hardening
28. Establishment of Countermeasures & Deterrents
29. The concept of If You See Something - Say Something
30. Social Media Monitoring Software
31. Solar Camera and Solar Lights
32. Formulation of Partnerships to Reduce Crime

33. Encompassing Effective CPTED Solutions in 2018 and Beyond: Concepts and Strategies
34. Community Policing: There is a Need for More Community Policing
35. Crime Prevention Through Integrated Problem Solving – A New Approach to the Broken Windows Theory
36. Cyber Security, Cyber-attacks and Ransomware
37. The Popularity and Need for Access Control
38. Fraud Issues: Large and Small
39. Social Media: The Good, the Bad and the Ugly
40. The Concept of Best Practices and Master Planning for all Properties and Organizations

41. Going Green – LEED
42. Digital Signage
43. Domestic Violence in the Workplace
44. Mass Shootings – Mass Casualties
45. Active Shooter/Active Assailant
46. Learning Strategies to Protect Soft Targets
47. CPTED Re-Invented (2018)
48. Cell Phone Technology Controlling Integration Issues for Smart Homes
49. Climate Change and Depletion of Natural Resources, such as Water
50. ASIS International and the International Foundation for Protection Officers (IFPO) Making Numerous Changes to increase Professionalism in the Security Industry

17 Points of HOW TO PLANT THE SEEDS TO SUCCESS IN THE SECURITY INDUSTRY

1. **Seek a Mentor**
   It's never too late to learn from an experienced professional.

2. **Earn a professional certification**
   Professional Certifications are looked upon more favorably than ever.

3. **Stay Focused**
   In this thriving industry it is easy to become distracted. Stick to your initial project.

4. **Listen and learn from your colleagues and peers.**
   As in any aspect of life but more importantly in your career. Learn from others.

5. **Network, Network, Network**
   Critical component is to gain a large network so that you may call upon subject matter experts, researchers, authors, etc

6. **Research and read**
   Keep current on emerging trends, guidelines and standards. Designate time daily to do this

7. **Healthy body, healthy mind**
   It's an old adage but a very practical one. More evidence has been published lately that the two are positive parallels.

8. **Explore various components of the industry**
   Though you might be involved solely in INFORMATION security it certainly would be beneficial to also learn other areas (example: Cyber-Security, Design Centers)

9. **Volunteer in leadership capacities**
   Not only does this introduce you to additional networking possibilities it also can enhance your CV/Resume. Most importantly you could be 'giving back to the industry'.

10. **Get published**
    Formalize your knowledge and expertise by writing an article or participating in a white paper publication.

11. **Be kind to yourself**
    Spend less time beating yourself up over mistakes, rather, view mistakes as learning experiences in your journey through life
12. **Do more than just show up**
    Be an active participant and contributor- get noticed
13. **Be a lifelong learner**
    Never believe you know it all, always remain open to hearing the opposing view
14. **Be the change you want to see**
    Adopt positive culture building
15. **Establish an ethos of selflessness**

Giving and sharing the credit establishes an ethos of selflessness

16. **Step outside your comfort zone**
    Learn new things or take on a new project that may be intimidating or daunting. It will stretch you in ways you never imagined.
17. **Your reputation precedes you**
    Maintaining a positive reputation and solid integrity is key to success in this industry

Footnotes:

*1 Bureau of Labor Statistics
Monthly Labor Review: 12/2013

[*2]The Top Ten Trends in the Future of Security, Institute for Global Futures, http://www.globalfuturist.com/about-igf/top-ten-trends/trends-in-security.html

[*3]When Millennials are the boss, CNN Money, 07/12/2017, http://money.cnn.com/2017/07/12/pf/jobs/millennial-boss/index.html

[*4]Mark Zuckerberg's 2017 Goals Shows How Millennials Want To Work, Forbes, 03/30/2017, http://money.cnn.com/2017/07/12/pf/jobs/millennial-boss/index.html

[*5]Allied Universal and Knightscope Tour Security Robots in Select Cities. http://www.aus.com/media-center/press-releases/view-press-release/articleid/1238/allied-universal-and-knightscope-tour-security-robots-in-select-cities

[*6]Ibid.Resources: *Academic and training programs

https://my.asisonline.org/Lists/AsisDownloads/ATP_Career_Opportunities_Security_2013.pdf