Special Feature

Healthcare security and safety: Past, present, future

Bryan Warren, MBA, CHPA, CPO-1, and Steve Nibbelink, CHPA, CA-AM

Newcomers in the field probably find it hard to imagine operating with little formal training, few tools, and no digital technology. In this special feature, pioneers who helped to turn healthcare security into a rigorous profession join with newer leaders to paint a picture of how healthcare security has evolved over the past several decades and where it is heading.

(Bryan Warren, MBA, CHPA, CPO-1, is President and Chief Consultant at WarSec Security, based in Gastonia, NC. Warren is a member of IAHSS.)

(Steve Nibbelink, CHPA, CA-AM, is Customer Solutions Manager at M3T Corporation, based in Mechanicsburg, PA. Nibbelink is a member of IAHSS.)

When the COVID-19 pandemic hit, everything changed: Suddenly, security officers were doing health screenings; PPE became incalculably valuable; and alternate care sites needed to be built and secured. Some practices have changed for good. The leadership displayed by security teams prompted us to reflect on how far our profession has come since the early 1960s, when security was often viewed dimly. To trace that evolution and help chart a course for the future, we asked leaders who began their careers in different eras about what the field was like when they joined, how it has changed, how they see the future, and lessons for newcomers. We are deeply grateful for their generosity in taking the time to collaborate with us. To highlight trends, we have grouped the answers to our questions according to when the

respondents first took their positions in healthcare security and safety. The numbers next to the respondents' initials indicate the year they entered the field. The answers have been edited.

RESPONDENTS

(in order of entry into healthcare security)

1960–1979

Russell Colling, CHPA, CPP, MS (Criminal Justice) retired from Hospital Shared Services, in Denver, CO, as Executive Vice President for Security Services.

Edwin W. Stedman, CW3 (USA Ret.), CHPA, was in the U.S. Army Military Police Corps.

Linda M. Glasson, CHPA-L (now CHPA-D) is retired. She was Security Manager at Sentara Healthcare.

1980–1999

Thomas A. Smith, CHPA, CPP, is President, Healthcare Security Consultants, Inc., in Chapel Hill, NC.

Bonnie Michelman, CPP, CHPA, MBA, MS, is Executive Director, Police, Security and Outside Services at Mass General Brigham, Inc.

Jim Kendig, MS, CHSP, HEM, is Field Director Life Safety Code Surveyors at the Joint Commission.

Martin Green, CHPA, is Manager, Security, Telecommunications & Emergency Preparedness at Baycrest Health Sciences, in Toronto, Canada.

Paul Sarnese, CHPA, CAPM, MSE, MAS, is Assistant Vice President for Safety, Security, and Emergency Management at Virtua Health Inc., in Marlton, NJ.

Russell Jones, PhD, CHPA, CPP**,** is retired from the Einstein Healthcare Network (in PA), where he was Director of Corporate Security.

Connie Packard, CHPA, is Chief of Public Safety at Boston Medical Center, in MA.

2000–PRESENT

Bill Navejar is Senior Sales Account Manager at Metropolitan Healthcare Services, in Fairfax, VA.

Randy Kolentus, CHPA, is the Reid Health Chief of Police, in Richmond, IN.

John M. Demming, MPM, CPP, CHPA, is Director of Operations at HSS, Inc., in Denver, CO.

Anthony ("Tony") Pope, CHPA, is Chief of Police and Emergency Management for the Columbus Regional Hospital Police Department, in Columbus, IN.

PEOPLE

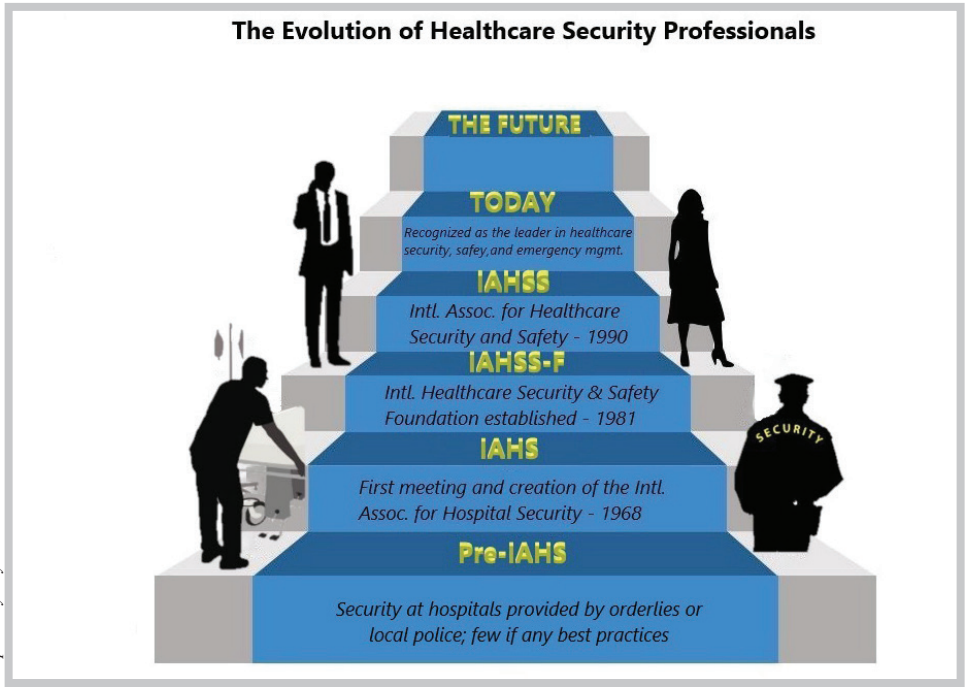
How did you start your career in healthcare security, and how big was your department?

STARTED 1960–1979

Russell Colling-61: While I was pursuing a master's degree in criminal justice at Michigan State University (my thesis was on hospital security), the school offered me the opportunity to consult on a project at Elmhurst Memorial Hospital, in Illinois. When the project was completed, I was offered a full-time position to implement a program as the director of security, reporting to the hospital CEO. The security staff consisted of myself, a secretary, a senior officer, and four security officers. This was at a time when there was little definition of the term *hospital security.*

Edwin Stedman-72: After I retired from the U.S. Army Military Police, I became the first chief of police at the Boston VA Hospital, a 14-floor inpatient and outpatient facility with an "old guard" attitude toward security. Security officers (without technology) monitored access and supervised open-lot parking. Watch clock stations guided building patrols. The day staff included me, a person for facility parking and access, and a person patrolling the facility.

Linda Glasson-76: I have never been in the military or law enforce-



Graphics by Bryan Warren

ment. I was hired into a hospital police department as an entry-level officer from another hospital department. My hospital had converted from contract to in-house. We started with 12 people, including the manager and clerk. My shift, the 3-11, had three officers.

1980–1999

Thomas Smith-81: I graduated from college with a double major that included law enforcement and security administration and a business minor. This odd combination qualified me for a security manager position at a community hospital in Saginaw, Michigan, which had 15 security personnel.

Bonnie Michelman-83: I was hired as a hospital security director through an ad after serving in corporate security. We had about 40 people (a proprietary department) with "contract" as a supplement. Technology was just beginning to come into play, and leaders in healthcare were not typically credentialed or trained specifically in healthcare.

Jim Kendig-84: I transitioned from law enforcement into healthcare in Pennsylvania. Much of my work related to safety (OSHA) and environmental (EPA); a minor part related to security at a corporate site and in emergency management. I later went to a two-hospital system as director of safety and security in Florida (included EM), which grew to a four-hospital system.

Martin Green-85: After studying law enforcement in college and working in loss prevention at a Toronto department store for seven years, I applied for a position with a small security guard company that was looking for a security manager at an undisclosed location. The location turned out to be a hospital in the west end of Toronto. I led a diverse group of 25 men, consisting of retiree's looking for something to do, newcomers to Canada, high school dropouts, and others. Not a single one had training or education in security. At that time in Ontario, anyone could get a security guard license if they passed a police background check and paid $40.00.

Paul Sarnese-86: I started as a part-time security officer at West Jersey Hospital, in Camden, New Jersey. Our campus included a large hospital, several primary care and outpatient facilities, and a school of nursing in a historically high-crime area. Most of my 50 or so fellow officers were retired men who were veterans of the Korean or Vietnam Wars. These were brave and proud men who taught me about security but, most importantly, about duty and service to others. That gave me great respect for their sacrifices and appreciation for those who came before me.

Russell Jones-87: I studied criminal justice at college before working in security for six years at Scott Paper and then taking a security director's job at West Jersey Hospital. The competition for the job was predominantly law enforcement. We had in-house security officers and used some contract services for supplemental support. After West Jersey Hospital, I moved to Hahnemann University Hospital in Philadelphia (once again, my competition for the position was law enforcement professionals). From there, I was recruited to Pennsylvania Hospital.

Connie Packard-95: I was working as a Sgt. for the Boston University Medical Center police when a merger was planned with Boston City Hospital; I got promoted soon after the departments merged. We had 40 officers, mostly special police. At the beginning, it was only one side of the campus with very few incidents. Most of our duties were escorts and/or access control and we were much busier than at the other campus.

2000–PRESENT

Bill Navejar-05: I started my career in healthcare security as a vendor, providing valet parking, garage management, and transportation services to medical facilities.

Randy Kolentus-06: I began my healthcare security career when I retired from our local police department after 28½ years. We were a 200-bed hospital with a behavioral health unit and a 24/7 emergency department. We had a small department of six "security guards" and me; two were 55-plus, and the others were in their late 20s and early 30s. There was only one officer per shift.

John Demming-14: My career began when I was a college student and went on a police ride with a friend. We responded to a call for an intoxicated person and transported him to the emergency room for evaluation. When we arrived, I saw a security officer in uniform and asked if they were hiring. The department had about 30 officers.

Tony Pope-16: I entered the field as manager of protective services and emergency preparedness at Columbus Regional Health after being encouraged to apply for the job when I was deputy chief of police at the Bloomington Police Department, in Indiana. We had one manager and 12 full-time employees as security officers (all non-sworn and unarmed). We also contracted with local law enforcement to provide a uniformed presence at our emergency department 12 hours a day during our high-risk times.

How were you or the department viewed by the clinical staff, the administration, and local law enforcement?

1960–1979

RC-61: The hospital staff was not quite sure how to view the new program. The ER staff was the first real support group. A primary task was setting up formal relations with the local police, who were happy to be called less often. I had been a police chief, which helped in our working with the local police.

ES-72: We were viewed with indifference. The VA Hospital relies on teaching hospitals for its medical resources, and the faculty and medical professionals exercised their status by not abiding by the rules set forth for all. The VA Hospital was exclusive federal jurisdiction; thus, local government authorities had no enforcement or investigative authority. The healthcare community took some time to get used to going from no federal police on campus to a formal police presence.

LG-76: We had just taken over from contract security and inherited their poor reputation. It took about eight months for our performance to earn the respect of the clinical staff, administration, and local law enforcement.

1980–1999

TS-81: We were viewed positively. Within a year of being hired as a security manager, I became the director of security and safety and had responsibility for disaster planning. The disaster planning aspect provided a lot of visibility within the organization and among the state and local law enforcement and fire departments. I was also the hospital representative for the planning for emergency response related to a nuclear power plant that was under construction. I ended up taking a role in the local planning groups, which forced me to make presentations to hospital and board leadership and to provide training for hospital staff.

BM-83: I developed a close relationship with the city's chief of police, which was helpful. I think we were also viewed positively because I put energy into cultivating relationships in the hospital and demonstrating a caring responsibility for my department and the varied groups and departments we served and partnered with. I tried to be very innovative, because much change was needed, and I involved many others by seeking their feedback, advice, and involvement.

JK-84: In the late 1970s and 1980s, we were not viewed as very professional, and the image of the old guard was on people's minds. Now security team members are very pro-

fessional and trained, and the appearance in many cases is crisper. There has been a transition from "guard" to "security officer."

MG-85: We were mostly invisible to staff, except when we tried to enforce rules. As for the police, there was no relationship at all. They viewed us as a nuisance.

PS-86: When I first started, we were called "security guards," and I believe we were perceived as rent-a-cops, not professionals. When we changed our title to "security officers," the perception of our significance began to change. We came to be viewed as an important part of the team. The majority of our officers lived in the community we served and knew the neighborhood and its residents, which gave us credibility with our customers and co-workers. We also had an outstanding relationship with the city police department.

RJ-87: I was responsible for more than just security, also for telephone operators, housekeeping, and parking. I tried to earn respect within the organization by bringing in the customer-service philosophy, engaging the community both inside and outside the facility, and creating and championing a different way of acting and communicating. Once you earned trust, you became a true partner (and, yes, nurses are the most important).

CP-95: Clinical teams appreciated the officers and the visibility we had assigned in the buildings and on patrol, and we always had good relationships with senior administrators, who saw our overall credibility and overall response.

2000–PRESENT

BN-05: When I first started making sales calls, I was viewed as just a "vendor." But I became more than that as I earned the trust of healthcare security and safety professionals.

RK-06: The leadership and administrative staff wanted to change what security had done in the past and were eager to accept new ideas and were very supportive. The local police were also supportive: they even gave us a police car that sat in front of our ED to provide deterrence. The clinical staff was eager for change but was less accepting initially because the past security department had not been as engaged with the clinicians as was needed. Now we attend nursing leadership meetings to discuss what we can do for each other to advance patient care and security.

JD-14: When I began as a security officer, I wore a police-style uniform. Later, we became "public safety offi-

cers" and wore a polo shirt top and eliminated police-style badges. I was almost always assigned to the emergency department, a Level II Trauma center with a psychiatric unit. There, I felt as though I was a valued member of the team. Even as an officer, I conversed regularly with medical staff and leadership. In situations where I needed additional help with restraints or dealing with a violent patient, the techs and RNs were quick to help. Working alongside police, you create a reputation for yourself, good or bad. As someone who cared about his job and took it seriously, I had the respect of my partner police officers.

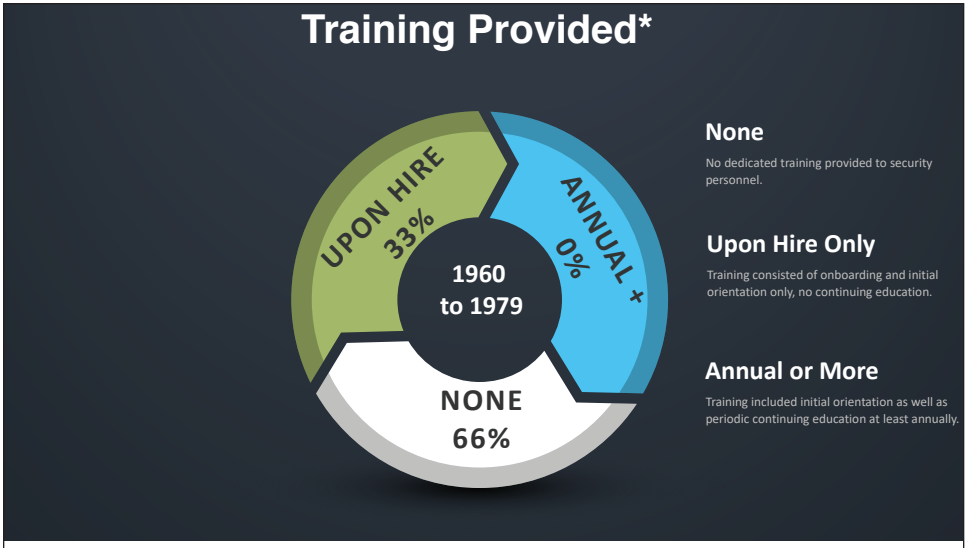
TP-16: Having worked closely with many of the local law enforcement officers and leaders, I already had an excellent working relationship with local law enforcement. Our clinical staff and administration really didn't know who I was at first, but it didn't take long for the organization to show me the respect and confidence that has allowed me to make some significant and much-needed improvements to our service model.

TRAINING

Describe your facility's security training program when you began.

1960–1979

RC-61: Training for the security staff was two-fold: Security operations (procedures) and training the security staff relative to healthcare departments and interface expectations. There was some classroom security training but primarily it was on-the-job training and one-on-one



*Percentages reflect interviewee responses to the survey questions.

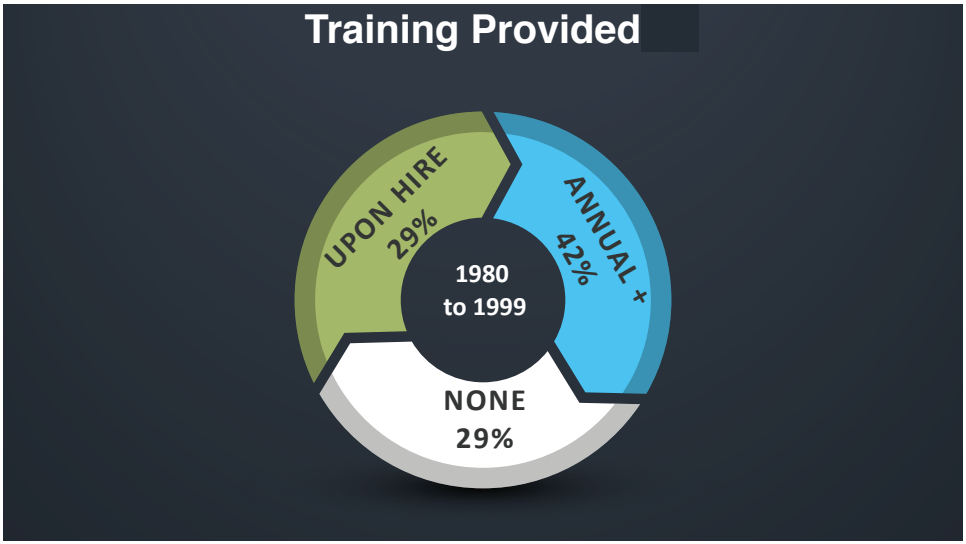
interactions because of shift scheduling. Later, we instituted a two-hour all-security-staff formal classroom training twice per month.

ES-72: After being at the VA, I moved to Boston University Medical Center as the director of security at University Hospital. Training at the time was nonexistent. As the chief of police at the VA, I had attended a formal two-week training program for Veteran Administration hospital police. However, security manuals were not immediately available at the hospital. The only security references were the first and second editions of Russ Colling's hospital-specific texts—they were critically beneficial. In addition, we had materials from the VA training program, and we adapted information from the military police crime-prevention and physical security programs to create a nascent training program. At first, we had Friday afternoon trainings once a month; these became more frequent as time went on. Activities and incidents, as well as "momentous" issues that occurred during the prior week, were reviewed, and resolutions were discussed.

LG-76: There was no formal training program, except that we were shown how to use the Detex clock for rounds and where the stations were. Training consisted of reading the departmental manual and if you were a new employee, a hospital orientation. Fortunately, I already had EMT experience and knew how to shoot a gun. Also, I was assigned to two partners who had served in combat in Vietnam; they understood the value of training and the concept of service to others and viewed force as a last-resort option. They showed me how to handle each function in the job description and had me demonstrate competency before they would "turn me loose." I had assumed that the job would be all action. Instead, I learned the importance of observation, listening, communication, documentation, and doing the basics well yet being well prepared for the few times all hell broke. At the time, we had to buy our own utility belts with holster, gun, ammunition, baton, flashlight, and handcuffs. My partners taught me how to use the equipment on my belt. They gave me a two-day training in how to use handcuffs and 10 days of instruction on how to use the baton from both the defense and offense perspectives. They took me to a firing range on our days off to make sure I knew how to use the gun and how to maintain and clean it, and they showed me how to retain the weapon if anyone tried to take it from me.

1980–1999

TS-81: There was little training at first: an annual 8-hour training class that included the typical orientation topic list for all hospital staff (fire



safety, disaster response, and so on). But we became an early adopter of the IAHSS Basic Security Officer Certification programs and then used the course outline to develop quarterly training.

BM-83: When I began, leaders in healthcare were not typically credentialed or trained specifically in healthcare. We had some competency-based training and de-escalation training, and we had on-the-job training. We built our own training and development program. I also was careful to hire people with excellent skills and attitudes and who wanted to really learn.

JK-84: Training was nonexistent at first, but that changed. We created a step program (modeled after the nursing step program and law enforcement's promotional process), in which security officers could move up the ladder (and receive financial incentives) by completing training and be promoted to C, B, and subsequently, A officer. The training included presentations by law enforcement and security experts, such as from the NCMEC, and on such topics as NFPA and OSHA requirements (for example, training on NFPA 10, relating to fire extinguishers).

MG-85: What little training we had was based around what key opened what lock, what time your lunch was, the location of the bathroom, what time we locked/unlocked the main doors. My staff also handled the operation of the parking booth in the garage, so training consisted of teaching staff how to manually calculate how much to charge for parking and how to break the wooden arm off the gate if it stopped working.

PS-86: I was assigned to a seasoned officer on each shift for a couple of shifts before I was able to work alone. We had an on-the-job training checklist that included all of the services we provided, our policies and

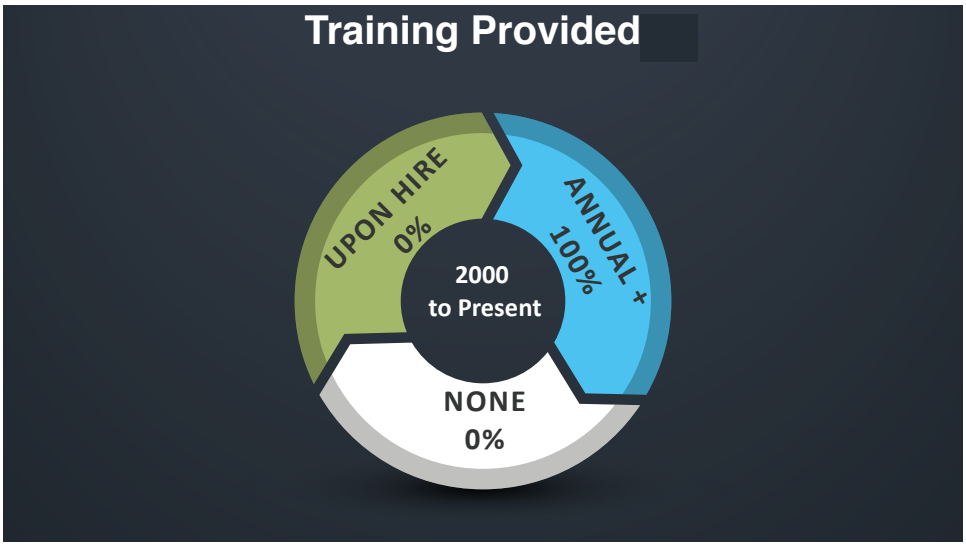
procedures, and the forms and paperwork that we had to complete. At the time, we were carrying handcuffs, mace, and a side-handle baton, so we had to go through several days of training on those pieces of equipment. We did have monthly meetings where we reviewed policies and procedures and received updates on organizational activities. We concentrated on the security functions, not really on fire safety, employee safety, or emergency preparedness, as others were managing those duties. I remember watching the Private Security Training Network VCR tapes.

RJ-87: Minimal, nothing formalized. The training was geared to hospital policy and procedure and did not involve de-escalation training even though workplace violence was prevalent. (We saw WPV training more in the 90's.) We only had orientation training when you were hired and then some annualized training for safety.

CP-95: Training was centered around Joint Commission compliance and renewals of our special PO licenses. We did provide annual training for de-escalation and duty belt equipment like handcuffs, pepper spray, and batons. As time evolved, more specific training and working with emergency management teams was implemented.

2000–PRESENT

BN-05: Mine was one of the first companies to have its managers in the IAHSS Basic Certification (once a week until certified, then ongoing). We started with 10 of our transportation and valet managers. They all became certified. As an organization, we adopted the IAHSS training philosophy, training standards, and best practices.



RK-06: We did not have a formal training program. We had to do the mandatory training designated by the state; our security guards would jump on a computer and do the modules. And they picked up what they could on their own. We were basically starting from scratch. We had no IAHSS materials or resources. A member of IAHSS who worked at the hospital in the transition period before I arrived showed me what I needed to do, and the steps to follow, and he pushed IAHSS and all the resources that were available. Our personnel liked their jobs and wanted direction and development. With one officer per shift, though, it was tough to do training, and no overtime was allowed.

JD-14: When I began in healthcare, on-the-job training was the foundation of the program. I was paired with an experienced officer or supervisor and was shown the workings of each post. I went through violence-intervention training, which was redone annually. At my hospital, security officers drove employee transport buses, which required me to obtain a commercial driver's license with passenger endorsement. I was also required to be CPR certified.

TP-16: When I arrived here, our security staff basically participated in annual training with our local law enforcement officers. This training gave the staff high-quality training in areas that included psychomotor skills like defensive tactics, driving, and handcuffing, as well domestic violence, human trafficking, and crisis intervention. This helped develop a professional working relationship between the security staff and law enforcement. However, after I gained a better understanding of the unique challenges and responsibilities of healthcare security versus law enforcement, I started to think of this training model as high risk. We were providing good training at a very low cost, but because our officers did not have the same equipment and authority as our law enforcement officers, it was not always relevant to their job or within the scope of their responsibility and ability and sometimes exceeded their authority. Not to mention that CMS and HIPAA required our staff to many times have a much different approach to interacting with our patients than local law enforcement does with the general public. I realized that we needed to change our training model to be specific and relevant to our level of authority, equipment, and scope. We now maintain a five-year training plan that is reviewed annually and updated and mandates monthly training topics that are in addition to the annual competencies required by the hospital. We also require that all officers successfully complete and maintain a certification through IAHSS's Progressive Training and Certification Program.

What were the most common training topics?

1960–1979

RC-61: At least half of the training was a discussion between security and representatives from various departments on how we could be helpful to one another, working as a team.

ES-72: Initially, training focused on patrol duties and the security director conducted all the training. For years, all security policies and procedures were autonomous and not in any type of formalized manual or compilation. What few physical security systems we had were either systems shared with security by clinical staff (such as the pager system) or manual systems; for example, access controls were lock and key only. In time, radio communications and CCTV video systems were incorporated into a 24/7 security operations center.

LG-76: Learning to use the equipment I had on the belt.

1980–1999

BM-83: Customer service, report writing, legal issues, violence, de-escalation. We did not have training in domestic violence recognition, and *cyber* was not even a word at the time—nor did we have sophisticated technology training.

PS-86: We spent a lot of time and energy on use of force and report writing. Everything was on paper, so we had many different forms we would have to complete, such as the daily activity report, incident reports, and time and attendance logs.

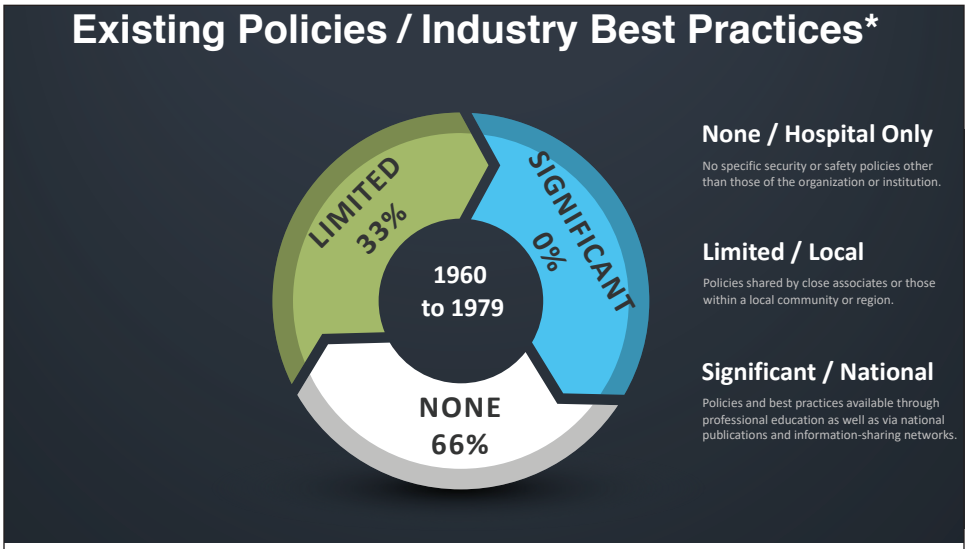
RJ-87: Customer service in dealing with the patient, report writing, basic investigations.

CP-95: Joint Commission, patient restraints, fire safety, de-escalation techniques, and report writing. New officers had six weeks of on-the-job training for their orientation with more specific response methods.

2000–PRESENT

JD-14: Crisis intervention and prevention, de-escalation, applying medical restraints, and learning the locations of the grounds. The majority of the training was on the specific workings of each post, creating visitor badges, patrolling, morgue input/release, and report writing.

TP-16: De-escalation, defensive tactics, soft and nylon restraints, and so on.



*Percentages reflect interviewee responses to the survey questions.

POLICY & PROCEDURE

Did you have written policies to guide the daily operations?

1960–1979

RC-61: In 1961, there were virtually no outside information resources to guide the development of hospital security policy and procedures. These were simply developed over time. ASIS was almost 100% government security.

ES-72: No.

LG-76: My first hospital manager wrote it based on hospital policy.

1980–1999

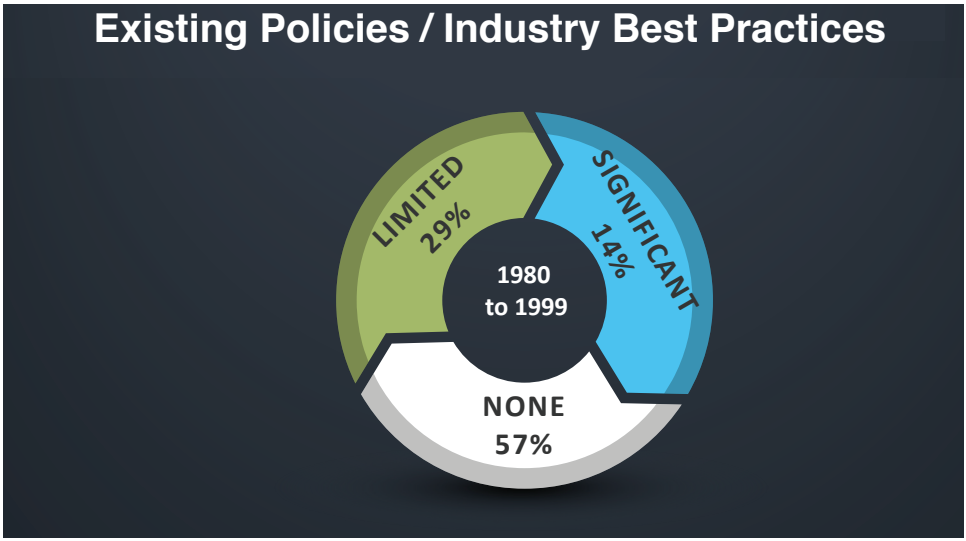
TS-81: I developed the first security department policy manual, with plenty of help from the person who was the director of medical education at the time.

BM-83: We had antiquated policies when I arrived; our team developed a comprehensive policy and procedure manual and also worked on a strategic plan for the department.

JK-84: Not at the start, but this evolved over time.

MG-85: No, other than what time to lock/unlock certain doors and how to handle morgue releases.

PS-86: We had post orders, general duties, and a code of conduct that was reviewed at least annually. We had a robust policy and procedure manual. When I became the manager of the department, we started a weekly in-service program, in which we reviewed one policy, procedure, or directive every week with the officers. This review took place at



the shift briefings. This was our version of the daily safety huddle.

RJ-87: We assembled a policy book—post, patrol, attire, hospital policies included.

CP-95: Yes, a written P&P manual and SOPs; the index had about 150 of them.

2000–PRESENT

BN-05: There were security and safety policies in place for security. We have developed SOPs for our different services in conjunction with the healthcare organizations.

RK-06: Our policies were old and not updated. We used some police policies as a starting point and reworked them to address hospital security requirements. Our organization and officers were very receptive to all the new ideas, very receptive to providing feedback and helping develop policy and procedure with the knowledge of what they did daily and the organization's feedback.

JD-14: I did not.

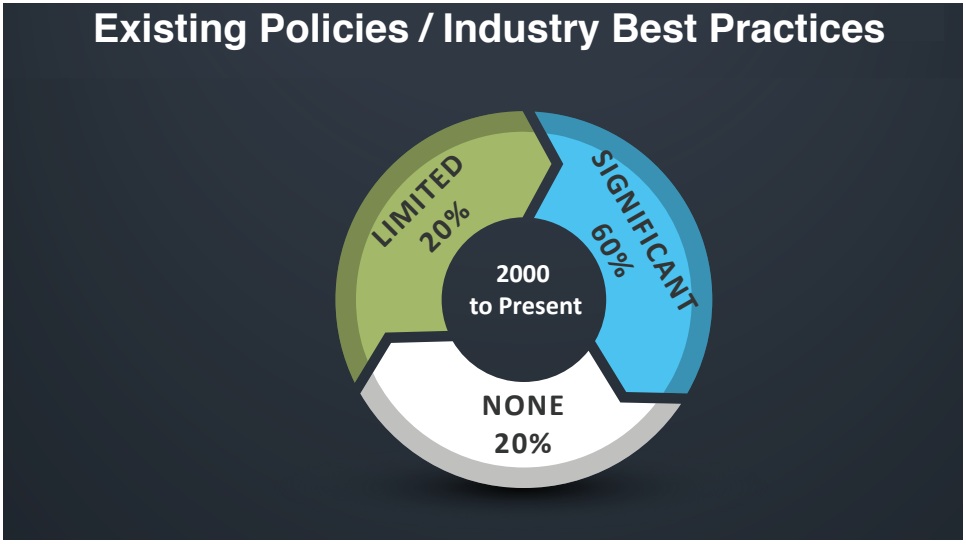
TP-16: Yes.

What references did you have to assist in creating policies and procedures?

1960–1979

RC-61: AHA had no information on hospital security. To create policies and procedures, I basically used my experience from my business college courses and from contacting various persons involved in hospital security.

ES-72: Russ Colling's *Hospital Security* text and the NFPA publications were primary sources. Within a few months, organizers of the Boston IAHS Chapter extended an invitation to a meeting; thereafter, we had great resources and colleagues



sharing knowledge and experiences. Materials presented during staff training sessions formed the foundation for publication of individual subject-specific security department standard operating procedures and special security instructions, essentially comprising policies and procedures governing service/mission expectations and performance.

LG-76: References were local and state statues, professional literature, and reaching out to colleagues. I had hospital administration, risk management, and legal review them.

1980–1999

TS-81: I used the IAHSS Basic Training Outline as a reference and begged, borrowed, and stole from anyone who would let me see their policies. I was also very involved in ASIS and used its published materials, my recent college textbooks, and of course, the first edition of *Hospital Security* by Russ Colling. Colling's book was dog-eared and footnoted everywhere as I developed our policy manual. I distinctly remember calling Russ for advice, which took great courage at the time! IAHSS members were very willing to provide input and assistance for a young colleague.

BM-83: We looked at other facilities to learn and share. We used our internal protocols (what had been agreed on by the hospital and its different groups), and we wrote our own policies and procedures. I worked regionally with IAHSS and used the policies and procedures from ASIS International member programs to interpret and transfer the knowledge to our healthcare program. I also benchmarked with other hospitals as well as other organizations and ensured I was in concert with regulatory requirements in the industry.

JK-84: IAHSS, colleagues at confer-

ences, state associations, relationship with local law enforcement (I was a law enforcement officer for 18 years).

MG-85: None. This was pre-internet and computers. I started out by searching for hospitals in the *Yellow Pages* and asking to speak to the "person in charge of security." That person ranged from maintenance or housekeeping managers to people in human resources or the nursing office, and sometimes "No one." When I finally got through to someone, I introduced myself and asked if they could mail something to me (this was pre-fax machines, too). People were very reluctant to share information that they considered proprietary or confidential. If I was lucky enough to get people to send me policies or procedures, I would review them and copy information that I thought was useful. In many cases, I had to write my own policies or procedures.

PS-86: I was blessed to have been mentored by Russ Jones. We had the *Protection of Assets Manual* and relied heavily on the IAHSS guidelines and publications to assist with developing new policies and procedures. We also used our network of IAHSS professionals.

RJ-87: Joint Commission standards at the time included topics such as the environment of care and safety but nothing related directly to the security function, which was a new concept for them. Security was seen as a non-essential department, thus creating a back seat mentality for our end user.

CP-95: To assist in creating policies and procedures, we mostly had JC and EOC or hospital/school requirements. Policy was designed for best practices but did not use IAHSS guidelines, as is done now. Unfortunately, new policies were changed or updated when incidents occurred; it was reactive rather than proactive. Now we review on annual basis.

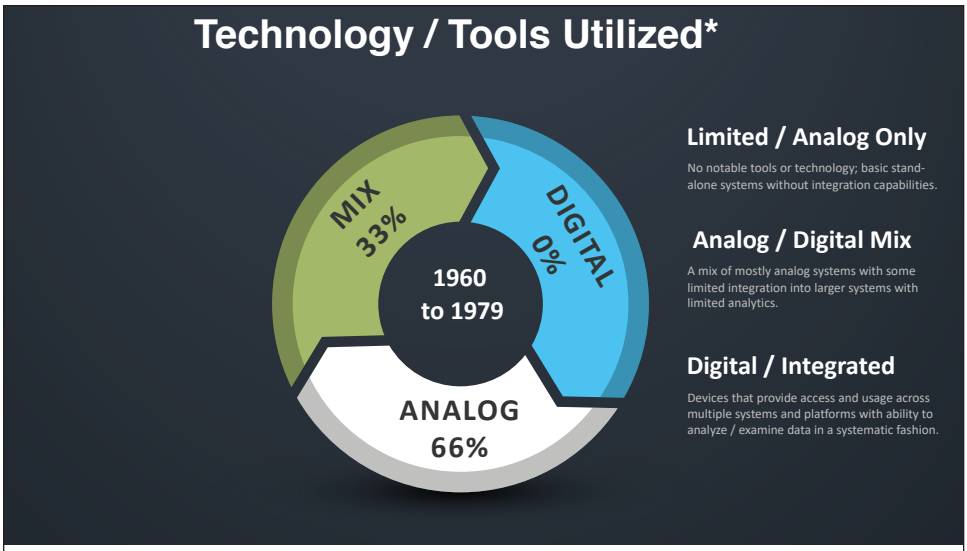
2000–PRESENT

BN-05: A combination of what we have developed over time, OSHA, JC, and our healthcare organizational partners. We started to lay the foundation with job descriptions, competencies, KPIs. Then we built the policies and procedures from there, and then created best practices. We went full circle and have a continual-improvement program to ensure we are up to date.

TP-16: The connections I have made through being an active member of the IAHSS have been invaluable. Members of our state chapter have been great at giving guidance and resources they have found useful. With access to the IAHSS website, I was also able to find electronic and printed resources that provided excellent industry best practices, standards, and guidelines. My main references

have been *Hospital and Healthcare Security* (*6th edition*), by Tony York and Don MacAlister, *IAHSS Healthcare Security Industry Guidelines, and IAHSS Security Design Guidelines for Healthcare Facilities.* I reviewed and assessed existing policies for inconsistencies in what the policy said and what we were actually doing. If our practice was consistent with our written policy, I would check it against industry standards, guidelines, and best practices using the resources mentioned above and make any needed adjustments. If there was an area for which we had no policy, I would typically network with my peers from our local chapter to discuss their practices and policy and then draft a policy combining our needs with the industry standards, guidelines, and best practices.

TOOLS & TECHNOLOGY



*Percentages reflect interviewee responses to the survey questions.

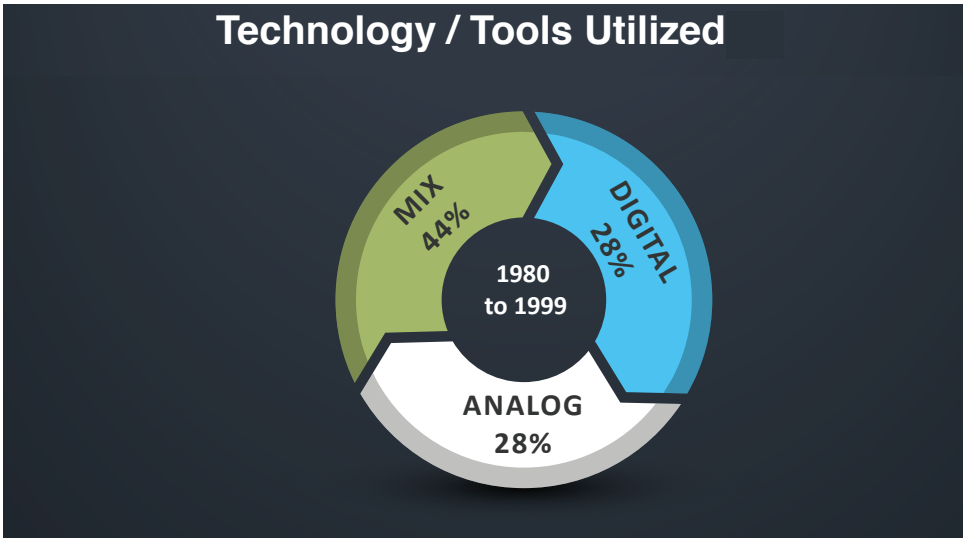
What tools were available to your security personnel early on?

1960–1979

RC-61: Very basic tools and very limited technology.

ES-72: Initially only a police-style uniform, subsequently replaced by blazer and slacks.

LG-76: Department officers had a radio, gun, handcuffs, baton, typewriter, cameras, video recorder, Detex clock, and a basic entry alarm system for perimeter doors.



1980–1999

TS-81: Time clocks (the old style), handcuffs, leather restraints.

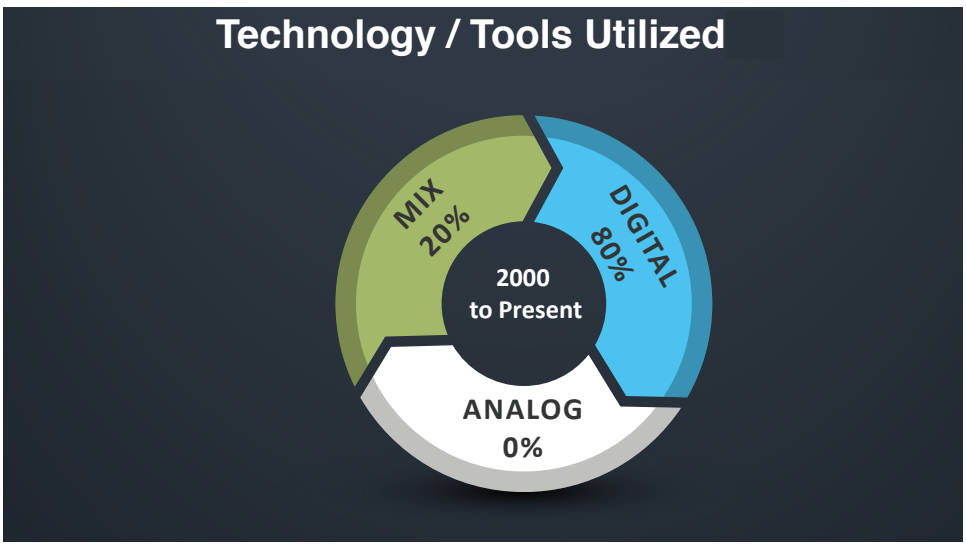
BM-83: We had some security technology but no defensive tools, although we did have handcuffs.

MG-85: Walkie-talkies.

PS-86: We had radios, keys, flashlights, handcuffs, pepper foam, and a side-handled baton. We started a K9 program in 1988. This has proven to be an invaluable tool and asset for our security program over the last 32 years.

RJ-87: A walkie-talkie and a flashlight.

CP-95: Handcuffs, pepper spray, batons, radios, and PPE.



2000–PRESENT

BN-05: Security personnel were in uniform and had radios.

RK-06: We had portable radios (in-house only that communicated with security, behavioral health, and the emergency department). We also carried mace, handcuffs, and flashlights.

JD-14: The only items I carried were a hand-held radio and flashlight.

TP-16: Our security personnel had uniforms, a utility belt, handcuffs, a radio, a baton, and pepper spray. We have body armor. The pepper spray is being re-evaluated as to if, when, and how we should use it.

What electronic technology was used in your security department?

1960–1979

RC-61: We had no radios. All calls for service went to the PBX, who used overhead paging to notify field security officers. No alarms for security (except for the fire alarm). No card or push-button function for locked doors. Some exit alarms, with the bell or signal at a door location (i.e., "break glass to activate"). Security officers on rounds used a key punch clock with the rounds report attached to their shift report.

ES-72: Initially, watchman patrol stations—the clocks. At first, we had a manual typewriter for generating an incident report. A few years later, an electric typewriter discarded by a clinical service provided an upgrade.

LG-76: During my first director's job, officers and departments had radios, pagers, cameras, and a basic alarm system, and there were a couple of duress alarms in the emergency department and psych. Our hospital didn't get a lot of technology during this time frame. We were aware of it though.

1980–1999

TS-81: Within the first year of my employment, we were directly involved in installing a state-of-the-art CCTV (old term) and access control system.

BM-83: We had video surveillance and management, access control, and panic alarms, and we integrated and functionally broadened our technology to our security program, starting with the first-ever Hugs infant-security system in New England.

JK-84: Initially a few card readers and basic CCTV. Eventually, we moved on to enhanced CCTV with motion action, access control, central viewing, parking area bollards, and

body cams. The list is ever growing.

MG-85: Other than walkie-talkies, nothing!

PS-86: We had a command center that had about 40 9-inch, black-and-white monitors that displayed one camera each. Each camera was connected to one of three video cassette recorders. We had a multiplexer that we could use to sequentially switch from one camera view to another view. We were innovative at the time, in that we were using quad monitors. One monitor could be used to view four cameras. Several of these quad monitors would be connected to multiple videocassette recorders. We had one cassette tape per recorder per day. We monitored an old bell-coded fire alarm system and the medical gas alarms. We did not have any access control system. All of our daily activities reports and incidents were recorded on paper.

RJ-87: Old analog tube cameras for CCTV and an identification badge but not a lot of access control. Technology was just beginning in the 1980's.

CP-95: Radios, access control with ID office programming, CCTV, panic alarms, blue call boxes.

2000–PRESENT

BN-05: Video, access, and alarms.

RK-06: When I arrived at the hospital, we had no electronic access control, only keys. At a certain time, our officers would lock the perimeter doors, with only the ED entrance being accessible. We had no video surveillance. Now, we have a newer facility. We have electronic access control and approximately 250 to 300 video surveillance cameras, and we protect 32 off-campus facilities.

JD-14: The most frequently used technology was video surveillance. In the psychiatric unit, real-time video monitoring was vital in watching several patients at a time. I would also use a handheld metal detector to make sure incoming patients were not carrying weapons or bringing other prohibited items.

TP-16: The technology was in good shape when I arrived. The alarm systems and video surveillance were in place; we are now looking at upgrading to up-to-date video surveillance technology. We had an in-house software system for records management/task and dispatch; it was hard to get reliable and relevant data out of the system. We have switched to a computerized incident management system. We are constantly working on how we can make all our officers better and more efficient in their jobs. We have installed mobile data terminals in

our vehicles; with the virtual connection, officers can write reports, gain access to files, view the video system, document activity, etc.

What were the major advances during your first 15 years or so, and how did they affect your role?

1960–1979

RC-61: A major change was the consensus that an in-house security force was generally superior to that of "moonlighting" city/county law enforcement officers. The advance of this concept was certainly slow moving.

ES-72: Introduction of personnel ID programs with the primary objective of understanding who populated the campus, particularly contracted/paid/unpaid staff, patients, visitors, volunteers, and vendors. Once elements of the campus population were identifiable, effective access controls were considered, and access points were established in order to to provide the best campus-wide entry/exit strategy. CCTV augmented access control. A central station was established to record access and for record keeping. Acquisition of integrated technology for security and telecommunications was a major advance.

1980–1999

TS-81: I remember the first PTZ cameras, with what I thought were amazing zoom capabilities. We also made use of some of the first proximity cards. I have been an early integrator of technology and have benefited greatly from early adoption of new electronic wizardry. Monitoring alarms, video, and staff from across the state or across the country is now possible and being done by many of our forward-thinking colleagues.

JK-84: Analog to digital CCTV… with motion…biometrics, access control, satellite phones, etc.

MG-85: Desktop computers were just starting to make their way into the workplace when I started. The program director that I reported to had bought a computer that was shared by six or seven different people or departments. It was not networked or connected to other computers. The computer was used for "word processing." Documents were saved onto a 5 ¼-inch "floppy" disc. The computer was connected to a "daisy wheel" printer with a "tractor feed" for paper. You could only save two or three documents on a disc. We were eventually notified that the hospital had purchased a "facsimile transfer machine," which was available for use (by appointment only) in the CEO's office for sending documents. The CEO's administrative

assistant placed documents that were received for us into our mailboxes. Early machines printed onto thermal paper that could not be copied or it would turn black from the light and heat of the photocopy machine.

PS-86: Some of the major advances in the nineties: Cameras became available in color. Access control systems allowed the employee ID badge to be used for access and time and attendance. My first system used an exterior mounted barcode that we placed on the employee ID badge. Electronic incident reporting systems became the norm as well. Our roles changed from managing the security staff and resources to managing security systems. These advancements required us to spend a lot of time and energy to learn the terminology and the systems.

RJ-87: We went from all-manual incident documentation to computerized reporting, including integration with video and an access control system as part of an overall program.

CP-95: Our department progressed from older, manual processes for incident reports to electronic systems, including upgrading from magnetic stripe ID badges to proximity card technology. This was challenging due to the learning curve related to computers; new technologies, such as biometrics and metal detection, are just being implemented.

2000–PRESENT

BN-05: Analog to digital, to the technology of today. Technology has become more user friendly and delivers better and more complete data for making better decisions for healthcare security and safety. Technology has revolutionized tasks; just imagine report writing a decades ago.

RK-06: The huge explosion of technology. The digital and connectivity explosion of healthcare and IT are all involved in access, video, and communications. The level of competency of our officers has grown, from focusing on keys to being knowledgeable about the current (and growing) state of technology. Our communications system is not just in-house, as it was in the past; we have 800 MHZ radios for communication with EMS and law enforcement. We have access to the prosecutor's office for ease and speed of communication.

JD-14: Video monitoring was a great way of documenting what occurred during an emergency. For example, we used past events to learn what went well and what could be improved in a use of force event.

PERSONAL

What were some major positive influences early in your own healthcare security and safety career, and how did they affect your later career?

1960–1979

RC-61: One key influence was the (slow) increase in hospital administrators' recognition of the importance of adding security and safety components. In addition, by introducing security as a service function along with deterring unwanted events, I earned a promotion path (from security director to assistant vice president for general services). The approach was also a major factor in my being selected to do a study relating the creation of a consolidated security system for a large hospital group in Denver.

ES-72: The medical center's institutional leadership served as respected mentors.

LG-76: The major influences were people. The two partners who trained me influenced my attitude about the importance and applicability of training. The nursing leadership emphasized the importance of people. Colleagues in IAHSS, many of whom were in ASIS as well, impacted my practice and knowledge base.

1980–1999

TS-81: I had three outstanding mentors. They included my college advisor Ken Fauth, Fred Roll, and my first boss in Saginaw, Joe Popovits. They all took an interest in me and helped advance my career by pushing me to do things far beyond my comfort zone. I must add my father to this group: the art of telling a good story helped my career in ways that were not predictable.

BM-83: 1) By working with my various bosses, who had different leadership and communication styles, I learned what did not work well and what I would want to see and be as a leader. In many cases, my team members and leadership were innovative: They stepped out of their comfort zone and encouraged me to take a chance and learn about change and moving people to new heights and success levels. 2) The associations I have been involved with have been a fundamental part of my growth, my success, and especially my enjoyment of my career. 3) Having a team of people that shares goals, engenders mutual trust, and makes continual progress possible even during tough times and events continues to be a source of pride and motivation.

JK-84: Having a law enforcement background, an advanced degree (masters), and networking.

MG-85: Connecting to IAHS (later, IAHSS) helped introduce me to information, people, and resources and fueled my curiosity; it became the single most positive influences in my career. After several years of being a member in name only, I was encouraged by then-president Tom Smith to become the first regional chairperson for Eastern Canada, where the number of members was under 10. Over time, membership grew to over 100, and we went from having no chapters in eastern Canada to four.

PS-86: Three people. My first supervisor, Ed Steinmetz, loved security technology. He sparked my fascination with surveillance, covert surveillance, and access control. He took the time to explain how cameras and surveillance systems work. I once even had the opportunity to crawl in the ceiling pulling a coax cable for a covert camera he was installing. I then had the tremendous blessing of working for Russ Jones. Russ showed me the potential growth opportunities in the field I had already fallen in love with. He stressed the importance of education and professional certifications. He is the role model that I want to emulate and continues to influence me today. During my first year in a leadership position, James Espinosa, who was our director of emergency medicine, and I shared the desire to improve security within the ED. We collaborated on research to identify best practices and collaborated on several articles about ED violence and strategies to mitigate violence. He spurred my desire to share my experiences and best practices through publishing research and articles.

RJ-87: I had a mentor who guided me as I made mistakes and learned from them. I also learned from the process of providing proactive customer service and working to contribute to the strategic mission and goals of the hospital.

CP-95: My career was influenced by receiving promotions and taking on more responsibilities, by learning the needs of the healthcare security program, and collaborating with other teams. I had a great leader, who was my mentor. Today. there is more mentoring and succession planning.

2000–PRESENT

BN-05: 1) Early in my career, I called Linda Glasson to sell her our services. She proceeded to quiz me on IAHSS and healthcare security. She made me want to know more and learn more, to be more professional, and to be of greater value to healthcare security professionals than just a vendor. 2). I also had the opportunity to meet Gary Switzer, who had a board in his office that had his entire staff, date of hire, and

date of completion of every IAHSS certification. Gary was one of the first security directors that attached IAHSS certification to employee compensation and increases. 3) The passion of all the people I have encountered (including healthcare leaders, presidents, and board members of IAHSS and the IAHSS Foundation) motivates me to share and give back; it is contagious.

RK-06: 1) The officers who were there: They accepted me; they wanted to move forward with change, grow, and develop. 2). The guy that trained me. He was only able to spend three days with me. He directed and guided me to IAHSS; he made the journey into healthcare security smarter and faster.

JD-14: 1) Roy Williams. When I was in college and started working in healthcare security, I became intrigued with the field as a career. I reached out to many people I had no connection with, such as security managers and professors, but I did not receive many responses. However, Roy responded and was welcoming and answered my questions. Here was the protection leader of an entire healthcare system talking with a 23-year-old security officer half a country away and, for example, giving words of encouragement and advice on a college major and career planning. 2) Alan Butler. Roy introduced me to Alan, who became another mentor while I was still in college. I would ask his advice on everything from a paper I was writing to where I saw myself in two years. In 2017, he gave me my first shot in healthcare security management, running my own program in Texas. 3) Tony York. I met Tony when I attended my very first IAHSS conference in 2018. I was a program manager at HSS, where he was the CEO. Tony took the time to coach and mentor me throughout my time as a young manager. One thing he taught me is that you have to love what you are doing, especially in this field. He is truly passionate about healthcare, and that passion has rubbed off on me. Tony has served as an example for me to follow.

TP-16: IAHSS was a major influence. I was so lucky to have connected with Randy Kolentus and Craig Whitfield in the Indiana chapter when I was making the transition from law enforcement to healthcare security. They provided mentoring and guidance while encouraging me to pursue my CHPA and the IAHSS Program of Distinction for my team. Along the way I also developed a solid group of peers to draw experience and wisdom from throughout the United States and Canada. Being active in my state chapter was the best decision I made in my healthcare career. Once I completed all three of the basic, advanced, and supervisor courses in the IAHSS progressive certification program, I felt strongly that this progressive certifi-

cation program made for a solid foundation of knowledge for our protective services department. I have updated all our job descriptions and made the IAHSS progressive certification a required certification.

What was the defining event in the world during your career that had a lasting impact on the provision of security and safety to healthcare facilities?

1960–1979

RC-61: It was a series of events that impacted hospital security over several years. One was the spearheading of awareness of infant security by the National Center for Missing & Exploited Children (NCMEC) (that is, John Rabun) and its provision of tools for hospitals to implement for preventing infant kidnapping. Another primary event was the recognition by the Joint Commission that security and safety were necessary elements of providing hospital care. Others included various major crimes, such as the "Speck" case (in which eight student nurses were killed in their shared hospital housing unit) and major infant kidnappings from hospitals. Also, the riots during the Chicago Democratic Convention.

ES-72: The means of communications changed and expanded; IT became stronger and more relevant, from data to the big picture. Also, in 1990, IAHS added the *S* for Safety, becoming IAHSS, and was involved with risk management and emergency management—growing in scope, vision, and contribution. The September 11, 2001, attacks occurred when I was fully retired; healthcare security had to immediately and forever adjust to the reality of national, regional, and local vulnerabilities previously not considered significant.

LG-76: The amount of violence in healthcare, infant abductions, and 9/11 all had an impact on day-to-day operations.

1980–1999

TS-81: Although not a defining event per se, establishment of the IAHSS Council on Guidelines has had a lasting impact on the industry. The work produced by this group, including *Healthcare Security Industry Guideline*s and *Security Design Guidelines for Healthcare Facilities*, has helped forge relationships with industry leaders and regulatory bodies impacting healthcare.

BM-83: There have been four defining events in my career. 1) A nurses' strike at Newton-Wellesley Hospital in the 1980s. Violence, sabotage, and other things occurred. 2) The first time we had a shooting at

MGH. It was a murder-suicide. An employee had behavioral health issues that no one had recognized. 3) The Boston marathon bombing. The events and the aftermath were the most stressful, difficult, tumultuous times in the history of this hospital and had a major impact on both MGH and the city. 4) The coronavirus pandemic. The pandemic has been challenging to people, morale, jobs, economic health, and physical health. We had to be agile with new functions, less proactivity, fatigue, frustration, and constant change.

JK-84: Civil unrest, for example around Rodney King (now a current area of planning needed). Pandemics, from H1N1 through COVID. Maturation of workplace violence issues, including preparedness, mitigation, and response activities, including active shooter. Working with law enforcement, including on pediatric abduction plans, etc. Forensic patient management and evidence.

MG-85: 9/11 was the first significant world event that changed security practices in healthcare. It certainly (for me at least) lead to a greater collaboration between our security colleagues; it became a conduit for sharing information. The second event was the SARS crisis that began in 2003. That had much longer-lasting impacts, as hospitals implemented active screening and visitor management. In my case, it was responsible for my obtaining much-needed upgrades to my access control system. These upgrades enabled me to better monitor and restrict access and better secure my facility.

PS-86: 9/11, a pivotal day for all public safety and security professionals. Everything changed because people didn't have the same sense of security and safety. That day reenforced that there are people in this world who want to hurt and kill innocent people. I can remember being at a constant state of readiness and crying every time I saw an American flag. That day pushed security into the spotlight and the national conversation. It was no longer seen as a cost center and an expense but a necessary and critical part of healthcare. I believe it changed how our country and the world viewed people employed in the security industry. Our industry became an important part in keeping places where we live, work, worship, and relax safe and secure.

RJ-87: In the 1990s, workplace violence and infant abductions. The abductions, averaging 15 a year from hospitals, led to the of writing guidelines for the NCMEC and use of technology to help protect the patients and families. Later, 9/11became a defining event.

CP-95: I have been in healthcare security and law enforcement for more than 30 years. The defining thing was strategic planning to

reduce risks and mitigation around incidents/events. Code Pink and Code Green (violence) were developed, and then, after 9/11, we got more involved in EM. We also planned for weather-related incidents and loss of power, etc. Today, we have worked on flags to be proactive when identifying violent patients or those who pose a risk. As a Level 1 trauma center in the City of Boston, we spent a lot of time working on protected patient protocols to keep patients and staff safe, as well as on collaboration with our law enforcement partners.

2000–PRESENT

JD-14: The behavioral health crisis. A 2012 report by the Treatment Advocacy Center found that the number psychiatric beds in the United States decreased 14% from 2005 to 2010. This significant reduction in mental health care has strained hospitals across the country. These patients often present at emergency departments, voluntarily or involuntarily. This poses a significant strain on caregivers. It also places healthcare workers in danger of becoming victims of workplace violence, which has greatly influenced how security programs are structured.

TP-16: The ongoing prevalence of violence against healthcare workers, the opioid crisis, and the COVID-19 pandemic.

What type of day-to-day issues did a healthcare security and safety professional deal with during your early years in the industry?

1960–1979

ES-72: Internally, we had limited support, guidance, and recorded precedent. (Policy, procedure, and training would have assisted in developing professionalism; negative events might have been avoided had more support and resources been available.) Externally, fixed posts were a waste of manpower; we had to develop a better method and practice to provide better service and more situational awareness. We did not have enough technology: door, video, communication.

1980–1999

TS-81: The issues are remarkably similar now: violence, hiring and developing the right people, reducing turnover, managing physical security and technology, elevating security awareness within the organization, showing the value of providing reasonable and appropriate security, gaining leadership support.

BM-83: When I first began in healthcare security and safety, we encountered violence, threats, stalking, bullying, intimidation. We still have all of this; it is just broader, more sophis-

ticated, and in different modalities.

JK-84: Staffing, which is critical to assure a safe campus.

MG-85: 9/11 didn't really change anything day to day, but SARS certainly did. The protocols and polices that healthcare facilities implemented for SARS were very helpful when COVID-19 surfaced.

PS-86: There is no such thing as a typical day in our profession. Every day is different from the last. Part of my day has always included rounding on our security officers and other departments and units. I want to be very visible and approachable, and rounding also gives you an opportunity to gauge the current stressors and activities occurring in the facility. Rounding gives you a great opportunity to speak to leaders and employees about upcoming new initiatives or projects to ensure they understand the "why" and the goal as well as the impact on them and the expected outcome. I learned early in my career that I cannot control what events I may have to respond to and how my time may be spent. I think that the sooner younger leaders understand that, the better their coping skills will become.

RJ-87: Infant abduction, WPV, and visitor control.

CP-95: A large amount of time on mitigating risks, daily assessments of vulnerabilities, and improving technology, training, and EM training drills, like active shooting and overall violence in the workplace.

2000–PRESENT

BN-05: Funding and personnel—healthcare security teams are truly forced to do more with less.

JD-14: The behavioral health crisis led to a notable shift in how healthcare organizations manage their mental health population, with new regulations on everything from screening to monitoring. Many security departments were tasked with managing these patients, which posed a new set of training and competency requirements for officers. This also strained many security programs by pulling officers away from other essential duties to act as sitters.

TP-16: As an example, we were expected to lock/unlock all the doors during the daytime hours. We obviously did not have the time to do this with our other responsibilities. Other departments are now primary for their own doors. Our officers offer support as a check in that we validate that the doors are secure as we do our after-hours rounding. If a door is left unsecured, we simply secure it and send a reminder.

FUTURE

How do you see healthcare security and safety progressing in the next 10 years?

1960–79

RC-61: I believe there will be further growth in healthcare security as it becomes further defined as an essential service.

ES-72: The complexity and nuances of 21st century security were never contemplated. Significant gains in science and technology will make it difficult for today's practitioners to maintain their expertise.

LG-76: I believe that if we are not careful, our humanity and compassion could get lost in the midst of technology and less human contact.

1980–1999

TS-81: Healthcare organizations will likely expect more from security leadership in terms of professionalism, quality, and return on their investment in security.

BM-83: We need to hire more competent, credentialed, strategic, business-minded and diverse professionals, particularly for our security leaders. We need to move healthcare security and safety much further along to incorporate our healthcare organizations into the whole healthcare culture, so that the C-suite takes healthcare security and safety seriously and we are part of the daily business operations and leadership discussions. Technology will continue to progress, but it should not replace people (and our intellect, training, decisionmaking, interpersonal relationships, communication, humanity). We cannot provide enterprise security with just technology or just training or just staffing; it is constant vigilance and commitment that make our efforts immensely valuable for our healthcare communities. We need to continue to grow the diversity in healthcare security and safety– throughout our teams! We need to get people from diverse backgrounds, education, and experience for the multifaceted challenges we face in the industry.

JK-84: More use of technology (CCTV, access control, others), increased professionalism of security officers, recent uptick in use of K9 at hospitals.

MG-85: Improvements to CCTV and other technology will continue and will be a major asset. However, I believe that the biggest need is for security guard/officer training and education programs. Security is no longer a necessary evil or a job for the uneducated or the retiree looking for a hobby. It is a profession, a calling, as important to a healthcare facility as its clinical staff and programs. Security staff need to be

properly trained and certified. I see a day in the future in which security managers are required to have certification to the highest standards. Perhaps there will be a college of healthcare security, the way that we have colleges of nursing, pharmacy, and other healthcare professions.

PS-86: I see physical security and IT security continuing to converge. We cannot install or manage an access control system, video management system, or other systems without the support of IT. More security operations centers (SOC) and network operations centers (NOC) will converge into one SOC/NOC, streamlining the need for resources and providing greater efficiencies and overall system situational awareness of internal or external events that could affect the organization. I also see more utilization of artificial intelligence and analytics to support our decision-making processes. There will be a continued merging of security, infection control, and building automatic systems to improve the overall safety and security of the facility. Every security system will be contactless and on our mobile devices. The use of biometrics will have much broader acceptance.

CP-95: Improvements in healthcare security training and professionalism through accreditation programs and advanced technologies to provide for better accountability, data tracking, and measuring; the possibility that armed officers with police powers may become more common.

2000–PRESENT

BN-05: The amount of exposure (both good and bad) on social media is immense: healthcare will be under the microscope more and more.

RK-06: As hospitals and healthcare systems continue to evolve, there will be a convergence of security and police programs in certain organizations, depending on the needs of the hospital, the leadership philosophy, and community acceptance. Healthcare systems are growing and converging so rapidly. The healthcare security/police leaders are very educated and experienced, which is changing the professionalism of the security/police officer role in our industry.

JD-14: I see an expansion of safety/security/EM leadership's responsibilities in healthcare. Especially during pandemic times when hospitals are facing financial hardship, leaders will be expected to take on more roles within the environment of care. I see an increase in these leaders' ability to manage finances and budget. I also see increased educational requirements for our leaders, with graduate-level degrees becoming more of the norm. From an industry standpoint, I see healthcare

security moving towards further professionalism in the field. As the IAHSS continues to grow and expand its training programs, I think we will see more proficient officers in hospitals. This will require further participation in these programs from healthcare organizations and contracted security firms. As our responsibilities continue to grow, I believe we will see increased officer training requirements from regulatory agencies like the Joint Commission.

TP-16: The use of sound and video analytics should bring some exciting opportunities for change in healthcare security.

What major challenges do you predict ahead?

1960–1979

RC-61: Security competing with all elements of healthcare to maintain healthy, progressive, and ample budget levels.

ES-72: Today's expectations of manpower, equipment, support, community relations, and colleague relationships could never have been imagined. Challenges include resource scarcity, funding, healthcare expenses, and a reasonable threshold of economic support for security and safety.

LG-76: The most important question is, What will healthcare look like in three, five, seven years? This determines our future needs as much as our hazard vulnerability analyses and assessments, etc., do.

1980–1999

BM-83: 1) The fiscal state of healthcare: What will happen to the Affordable Care Act? Baby boomers require a lot of healthcare. There are not enough healthcare facilities for specialty needs, and behavioral health services and care are inadequate. 2) How will hospitals be reimbursed? This is a key challenge to properly sourcing and performing our healthcare mission. 3) Diversity in healthcare leadership and qualified employees. Benefit and compensation need to be structured to retain compassionate and dedicated professionals in healthcare.

MG-85: The biggest obstacle is and always will be financial. Sometimes it's very difficult to prove a return on investment for a security initiative.

PS-86: The financial impact of COVID will be felt for several years, and many organizations may not fully recover. I believe that there will be more mergers and acquisitions, and larger integrated health

systems will be the norm. There will be competition for resources, and we will need to continue to demonstrate our value every day. We need to be able to capture data that is relevant to the goals of the organization. I also believe that we will continue to have our resources stressed as care is provided for those dealing with mental health and addiction issues. The legalization of marijuana will also create unique challenges in our hiring practices and how we manage our customers.

RJ-87: Budgets are always going to be an issue (more with less), competing for the capital and operating dollars. Regulation will continue.

WPV will continue. We will continue examining how to use technology to be a better program and whether you can replace a person with a piece of technology.

CP-95: Workplace violence and the pandemic have certainly hurt healthcare facilities financially and can impact support services like security. IT issues, such as ransomware, are also affecting HCFs. Also challenging are weapons entering our hospitals; metal detectors to combat this are always being discussed and can be very challenging in large medical center environments. We review with senior leadership as needed.

2000–PRESENT

BN-05: The main challenge will continue to be funding.

RK-06: The teaching and educating of our administrative teams about what healthcare security (and PD) does daily is an ongoing challenge, as is helping our healthcare community recognize the need and the value we provide. (After all, our return on investment is not typically the same as that of the surgery center).

JD-14: The biggest challenge we face as an industry is the perception of our profession. We must continue to combat the impression of the "corporate cop." To accomplish this, it is imperative that we drive the industry in two ways. One, we must further establish ourselves as industry leaders by creating a consultative relationship with every healthcare association, accrediting body, and university we can find. Sharing IAHSS guidelines, pursuing authorship in multidisciplinary/academic journals, and building lasting partnerships will cement our position as a valued partner in healthcare. Two, we must increase certification and education requirements for all practitioners within our industry. We need to communicate the importance of certification attainment for manager-level employees and urge healthcare organizations and security firms to require them upon hire.

TP-16: The prevalence of workplace

violence by patients and visitors against our nurses, physicians, and ancillary staff must be addressed. What we have been doing in the past is not having the desired impact across the board. We clearly can't maintain the COVID-related levels of access control and visitor restrictions; it is not in the best interest of our patients in the long run absent a disaster or pandemic. However, I do not feel we can revert to the porous, largely uncontrolled, and vulnerable environments that existed before the pandemic. Our challenge is striking that reasonable balance of controlled access and visitor management that allows us to protect our patients, visitors, and staff while maintaining a healing environment that allows our patients to have a reasonable amount of support from family and friends.

What key lessons have you learned, and what advice do you have for others on this path?

1960–1979

RC-61: Do not be all things to all people, but always look for new challenges, even though it may not be within the traditional arena of the so-called security definition but does contribute to excellence in the delivery of healthcare services.

ES-72: Lesson: You have to know the beast. Advice: Increased education in all aspects of security, safety, technology, communications, and IT.

LG-76: Listen to, respect, and learn from others.

1980–1999

TS-81: Pay attention to mission and culture. Align your goals with that of your organization; make sure the culture of your department is supportive of the overall mission statement of your organization and that your staff members know how they help your organization meet its mission. Use metrics proactively to show your value to the organization. Maintain relationships: If you do not have positive, solid relationships with your core customers (usually the leaders and staff in the emergency, psychiatry, human resources/employee relations, and legal departments and the senior leadership staff of your organization), your department is in danger of being changed, outsourced, or redirected in a way you may not appreciate. Continue to elevate the professionalism of your organization. Not too long ago, the security department "chief" was a retired police chief or someone from federal service that looked for a job to supplement his retirement. Today, most senior leaders of successful HCF security programs have advanced degrees and certifications such as the IAHSS Certified Healthcare Protection Professional and have worked

many years in the healthcare security business. Our officers today also require advanced training, such as that provided by the IAHSS general, advanced, and supervisory certifications. A recent enhancement is the IAHSS Department of Distinction status, awarded to hospital security departments that maintain high levels of certified officers on staff.

BM-83: 1) Blend intellectual, social, and emotional intelligence: know how to compromise and connect, listen, communicate, and think strategically. 2) You cannot pick or even win every battle: You may not get what you need or want; you need to be creative and ask for help. 3) This is a remarkable field with a great mission. If you feel like you are getting burned out, get help or get out. Be full of energy, engagement, and passion. Always try to stretch your learning, standards, and capacity. Learning in different modes is critical. 4) Be a mentor, have a mentor. This is a high-stress profession. It can be tough emotionally. Leading people is not for the weak, but it is so rewarding; help others to maximize their ability to succeed and the organization to succeed.

JK-84: Find a mentor. Copy and improve best practices. Networking is key in the industry and community, including the law enforcement community.

MG-85: Never stop learning. No matter who you are or how long you have been doing this, there is always something new to learn.

PS-86: As security professionals, we must know our book of business (financial performance, key performance indicators, and benchmarking data) so that we can speak to our strengths and opportunities for improvement. As safety, security and emergency management professionals, we must be prepared to support the entire organization, not just the hospitals. We should support homecare, corporate offices, and other nonhospital functions, showing the expertise and value we bring to the entire organization. We need to invest in our own knowledge and education and take advantage of the many resources offered by IAHSS.

RJ-87: You will be able to do so many things if you have a customer service philosophy. Sell your program, for funding, investment, and growth; market your program every day to your staff and in-house and external groups; and know your customers. It is OK to fail: You will fall down, and people will help you back up. Have fun and enjoy the moment. We have been blessed to be on this journey to help our industry and one another.

CP-95: Have security leaders get out there and see the job; know your team so they can see your support. I refer to it as MBWA: Manage by walking around! Network as much

as possible internally and externally to see what others are seeing and doing; we need to share those best practices more often. We may make mistakes, but how you recover is what will be remembered; so, continue to be proactive and not reactive. If possible, take the time to make it right! Be a member of IAHSS: great networking and excellent resources, like the guidelines and other published materials.

2000–PRESENT

BN-05: If you are new to the healthcare security and safety field, ask questions and educate yourself. Train, train, train. Get involved with IAHSS: Relationships and networking are key to your learning and education. IAHSS has plenty of resources and its members are eager to share best practices. Just ask!

RK-06: Education, education, education: The more you can get, the better. It makes you more marketable; you can do more; and you can connect more easily with other people. IAHSS is the only organization specifically focused on healthcare security and safety. It should be in every facility! If you do not take advantage of its people and resources, you are doing yourself and your healthcare community a disservice. Always take advantage of the professional members and their passion to give back, share, and continually learn and grow. Also, be a bigger voice in the C-suite, providing understanding of what we do and the value we bring to our healthcare community.

JD-14: You cannot go it alone in this field. It is important to seek advice from others willing to help and to learn from those with experience. Also, healthcare is ever changing: Every year there is a new standard, practice, or guideline. You must educate yourself on these changes to stay ahead. This is a demanding field. You will be tested and will face challenges. The duty of protecting our caregivers is not a responsibility to be taken lightly. However, you will not find a more fulfilling career. Find your passion in life and relentlessly pursue excellence in all that you do.

TP-16: This is not a career in which you can afford to be a lone wolf and try to do it on your own, no matter how great you may think you are. If you operate in a vacuum, you are setting yourself and your organization up for failure. The IAHSS is the place to start. By getting involved at both the state and international levels, you will surround yourself with the best in the industry. I have found that the members at all levels care and want to help one another succeed.

OTHER

Do you want to add any other thoughts?

1960–1979

LG-76: I'd summarize the history of the field like this…
1970s. Usually, you relied on the training you received before retiring from the military and law enforcement. Regardless of whether you were a manager or officer, you received little to no training. Formal training was hard to find. The realization dawned that this was a profession in its own right.
1980s. Some training programs were starting to evolve locally, basically classroom and on-site training, and some seminars. Literature was beginning to become available. Vendors who installed equipment for security in hospitals would provide training on the equipment and its use. Equipment: cameras, video recorders, radios, beepers. It was hot stuff if you had an electric typewriter.
1990s. Word processors, computers, robotics, internet, and Wi-Fi were starting to be used. Radios and pagers were still commonplace. Use of the internet for training potential increased, and there was more networking among professionals, departments, associations, and other disciplines. We had more training opportunities and more training manuals for security, hospital security, healthcare risk managers, and safety and emergency managers. There was increased emphasis on professionalism for healthcare security, be it manager or officer level. As budgets continued to tighten, we had to become more creative with staffing, equipment, training, and certifications. We truly began to see the value and potential of the digital world and evolving technologies and incorporate them into our practices, including using cell phones and interactive computer training.
2000s: Our profession is using robotics, nanotechnology, artificial intelligence, analytics, programs to analyze the analytics, and remote communications technology. *Key lessons:* Listen to others. Respect them. Learn from them.

1980–1999

PS-86: Thoughts on leading your team:

- Surround yourself with diverse, multi-cultural, multi-generational, talented people who think differently and bring different skills and talents to the team.
- Put the spotlight on your people. Let them get the recognition and kudos for accomplishing a task.
- Everyone on staff must embrace the concept of "we" and "team" Build a team that supports one another and enjoys the success

of the team over individual success.

- Seek others who complement your talents or push you to look at things from a different point of view. Before you think about "how" you can accomplish a task, think about "who" needs to be involved to achieve success.

CP-95: In these times of COVID-19, civil unrest, upticks in violence against healthcare workers, and quality-of-life challenges (homelessness, substance use disorder, mental health), be prepared to recognize burnout and compassion fatigue stemming from the issues mentioned and have a plan for providing assistance to those affected.

2000–PRESENT

BN-05: The IAHSS Program of Distinction is huge and a very valuable asset and tool, as it shows how much your department and organization care about the community (both externally and internally). It is a winner for the community, the employees, and the security and safety team. Also, all security directors should do their best to complete the IAHSS Foundation's crime survey each year.

JD-14: I believe the future is looking bright for our industry. We will continually increase our impact on healthcare through the dedication of our leaders and under the guidance and mentorship of our predecessors.

TP-16: In making the transition from law enforcement to healthcare security, you are moving from crime fighter to peacekeeper. To be the best in our profession, to serve our hospitals, we cannot work alone. We need to network, be part of associations like IAHSS, and ask questions; we need to learn from others to see how they have dealt with the same challenges and found solutions.