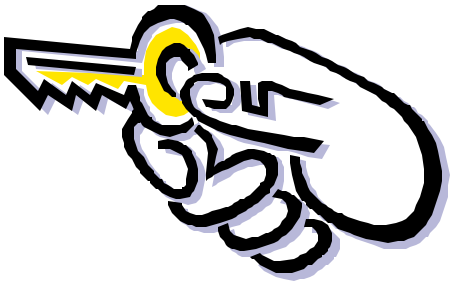
TECHNOLOGY: UNLOCKING THE FUTURE FOR SECURITY PRACTITIONERS



BY STEVEN R. KELLER, CPP

For many years, the security officer was a mere watchman, or a potted palm, stationed in a lobby to watch the comings and goings of all, without much authority to act. His boss was a building superintendent, another guard, or perhaps a bureaucrat who lacked much understanding of security as a profession. Under the best (or worst) conditions, security personnel had only to be "toughs," physically better than those they "policed." Those with brains need not apply for the position, and the most complicated piece of equipment the security practitioner had to operate was a door lock.

Within the past twenty-five years, a new generation of security manager has developed, and organizations such as The American Society for Industrial Security have been born which advocate higher standards and certifications. In the early days however, the security manager was still a second class citizen, so to speak, within his organization and lacked any real role in the general management of the firm.

I was a super-achiever. After a very active five years on the Washington, D. C. police force, I joined a federal government agency as a Special Agent and was soon placed in the position of Assistant Director of Security for the entire agency. I recall discussing career options with a friend in the Personnel Department and was told that I should not bother to apply for openings outside the security operation, since security personnel were "earmarked" as being unacceptable for general management positions no matter how talented or successful they were.

That same year, I spent $145 (a pretty good sum for someone who took home $175 per week) for my first electronic calculator. It was small, but twice the size of the typical calculator most of us own today. I don't know why I needed it, but I knew that I had to have one. Even my departmental budget was done for me by a bureaucrat who knew more about my operation than I did--at least in the eyes of my superiors.

The revelation that I was on a dead-end career path and the purchase of one of the first pocket calculators, were related. During the next year, my agency had lost hundreds of small calculators off desks, their small size making them vulnerable to the cleaning crews and the deliverymen who stole from

Steve Keller is a security consultant specializing in museums, cultural institutions and historic sites with headquarters at
555 Granada Blvd.
Suite G-3
Ormond Beach, Florida
32174
Tel. (386) 673-5034
Fax. (386) 673-5208
E-Mail steve@stevekeller.com

offices daily as they moved through the Washington, D.C. labyrinth of buildings. But it really didn't matter. Within months, the calculators were outdated, replaced by increasingly less expensive models until a typical credit card-size calculator replaced all of the high-priced, less powerful models that remained.

The year the calculator began to shrink marked the beginning of a revolution. The technological revolution, that is. It was a whole new ballgame! Along with the explosion of technology came the explosion in security technology. I no longer wanted to leave the exciting field of security electronics and technology. I wanted to grow with it. The growth potential was, and still is, unlimited.

Looking back at my peers, men and women who had left the police department in the mid 1970's to pursue security careers, I've noticed that although some made the "big time" solely on their management expertise, most were displaced by a whole new generation of security practitioners who knew their way around a computer and had a sound basic understanding of other aspects of technology. Today, when I look at those who are "making the big bucks," I see that most have at the very least, kept up with basic security technology. But what I see beyond the current generation of security managers is a generation that has mastered some advanced areas of security technology and have a sound basis of understanding of many others.

So what does it take to be a success in the new era of security? While there is still an emphasis on management, a well-rounded security practitioner will have to keep ahead of the technological revolution and its security applications. Security managers are increasingly becoming part of the overall corporate management team. They are expected to know about the business of the business they serve. That means that if you want to be Director of Corporate Security for an airline, you had better learn about how airlines operate. In any case, you better know how to read a corporate annual report. Probably most important in the management area is the need to be articulate, orally and in writing. If I were hiring a security manager today, I'd want him/her to be a business person who had made a successful transition into security, then moved up the ranks gaining practical experience in management and security technology.

What technical skills are needed? Unless you pursue an electrical engineering degree, colleges really don't teach many security technology courses! If you don't know how to operate a personal computer the day you enter the security field, you don't have a prayer of having a successful career in security in the coming years. Students interested in entering most careers today had better master one of the major integrated software packages, which include a wordprocessor, data base, spread sheet, and modem communications package. Students should know personal computer hardware, too. If

you don't have a basic understanding of what a computer is and how it works, you're in big trouble before you begin.

Why is this so critical? Not only is the modern security manager expected to manage, he/she is expected to do spread sheet analysis of budgets, loss projections, pay raise analysis, etc. He/she must prepare memorandums requiring more than basic wordprocessing skills, and he must completely master a variety of data base skills to enable him to use the power of a computer to his advantage as a manager. Gone are the days when incident reports can efficiently be kept on paper or scheduling done on an old fashioned legal pad. Investigative files occupy a data base and even disaster plans and call-up lists are computerized. Of course, the personal computer is also becoming an important component in the alarm and access control systems in use today. The best way to be regarded by your boss as the "Lead Guard" or to be earmarked as inadequate for company management is to fail to learn to use the power a computer allows us.

The security practitioner of the present and future must know the latest in security equipment. Subscriptions to the major security magazines and journals are critical. Many old-time practitioners make the mistake of reading only materials that interest them. The successful practitioner will read everything he can get his hands on, especially the ads! On a daily basis, the successful security manager will read the *New York Times* and the *Wall Street Journal*. On a monthly basis, he will read *Security Management*, *Security*, and as many of the other more specialized security publications as he can, such as *CCTV* and *Access Controls*. If there are security newsletters in your field of specialty, subscribe to them. *Hotel/Motel Security and Safety Management* and their counterpart newsletters for college and hospital administrators often have in-depth discussions of technical and non-technical matters. The general management "trades" as they are called, the monthly magazines directed toward non-security managers in your field, such as *Museum News*, *The Journal of Property Management* or *Shopping Centers Today* are essential reading.

I am a collector of what are called in the security and building industry "catalog cut sheets." Catalog cuts are advertisements for various products, such as components of security systems (motion detectors, alarm panels, locks, etc.) They also contain operational data and specifications. There is hardly a security product available, or that has been available in the past 10 years, that is not on file in my office in the form of a cut sheet. I am an avid user of "reader reply cards" found in most security journals, and I attend security trade shows as often as I can, specifically to gather information on security products and equipment.

If I don't understand a particular product after reading the cut sheet, I ask someone who can explain it to me.

I've received most of my technical security knowledge by asking the right questions of the right people. When I attend security trade shows, I try to catch the most important seminar programs, but unlike many of my colleagues, I save time for a thorough review of the exhibits. In fact, I often spend days in the exhibits. When most attendees are in the seminar, I'm spending time with the representative selling a product that I want, or need to know about. I plan my time in the exhibits when everyone is in a seminar, so I don't have to compete with too many others.

When I approach an exhibit booth, I ask "Who's the salesman here?" That's the guy I don't want to talk to. I also don't want to talk to the pretty model hired to spew out a canned sales pitch about the product. When I've identified the salesman, I seek out the technician and let him explain to me what the product is, and how it works. Now that's how you learn something!

There are several major areas of security technology that are especially important to know. They are:

1. Large security systems. These systems are computer-based, meet high security "standards" as defined by Underwriters Laboratories (UL) or the Department of Defense (DOD), and often integrate burglar alarm, fire alarm, access control, CCTV, and related systems. They are designed for large installations or very high security situations.

2. Small alarm systems. These are generally referred to as "alarm panels," but also include affiliated control equipment, such as digital communicators that transmit an alarm signal to a monitoring site. The variety of alarm panels is great, and the security practitioner must know the correct application for each type of panel.

3. Interior and exterior alarm initiating and alarm indicating devices. Initiating devices are detectors, from switches to motion and sound detectors, that catch the crook. Alarm indicating devices report the catch to the alarm panel or computer by doing something. Simple alarm indicating devices are bells or horns, and more sophisticated indicating devices are limited by the imagination. The various alarm components are the basis of most security systems. Understanding the various technologies of detection such as infrared, microwave, ultrasonic, sound discrimination, and verified technology, to name a few, is absolutely essential. One must know how each technology works, the causes of false alarms for each technology, and the best way to apply specific detectors and alarm indicators in specific situations.

4. Fire Systems. Know everything you can learn about fire systems. As the role of the security professional expands, it expands into the area of fire protection, safety and risk management. Fire systems, like security systems, use alarm initiating devices and alarm indicating devices, and you must know the best application for each. Not unimportant is the need to know about fire suppression systems. While it is not as important for the security professionals to have the depth of

knowledge regarding sprinklers, extinguishers and similar suppression technologies, a broad knowledge is useful. Increasingly, we become "protection" professionals, not just "security" professionals.

5. CCTV Systems. Closed circuit television cameras, monitors, mounts, recorders, enclosures, lenses, and related equipment are important knowledge for us all, as CCTV is playing an important role in modern security. Learn about the means used to transmit TV images, such as fiber optics, microwave, and various hard wired technologies. Learn about digital transmission of TV signals. Slow scan television and transmission of CCTV signals over phone lines, by radio signal, and over alarm wires is the trend of the future.

6. Locks. Know about locks, both mechanical and electronic. Know about access control systems, including electronic door strikes and magnetic release locks. Know about card key technology and biometrics. Know about key control and key control equipment. A full understanding of the electronic access control technology is a must in most corporate environments.

7. Security Communications. Know how alarm signals are transmitted. Know the technology involved and the equipment required. Know how alarm signals are defeated in transmission.

8. Security Containers. It is important to know about cash boxes, key boxes, safes, and vaults. Know about weapons cabinets, document destruction systems, and document waste disposal products. In security, there are a vast number of instances where you must protect valuables by containerizing them. You cannot perform this responsibility if you do not know the vast market on secure containers.

9. Fences, glazing, hardware and barriers. Learn about bullet resistant glass, hollow metal door products, and fence protection systems. Know what the market holds today and where it seems to be going in the future.

10. Understand security electronic systems. Battery backup units, generators, power supplies, and transformers.

Of course, there are other areas that are important, but the above will get you started. Learn as much about these technologies and the related equipment as you can by introducing yourself to the products in catalogs, in journals, and on display in trade shows.

Knowing about security hardware and technology is not enough. It is important to know security standards as well. Read everything you can about Underwriters Laboratories, Factory Mutual, and similar technology standards. Ascertain what standards apply to a specific technology and learn what the standard requires. You can get this information by discussing standards with the manufacturer of a product, then reading the standard

itself, available from the standard setting organization.

Learn about the National Fire Protection Association and their National Fire Codes. Fully understand the Life Safety Code, also distributed by the NFPA. Many of the logical security countermeasures against crime in a facility are not available to us due to fire code restrictions that facilitate quick egress in an emergency. There are other codes and standards, as well, that affect security. Standards for lighting, for example, are critical. And then there are the de facto standards. A number of legal case law newsletters are available which outline current trends in security litigation and serve as de facto standards on how much security is legally enough in a particular environment. Light levels, alarm requirements, etc. are all affected by court cases.

The modern security professional must understand how security can be designed into a building during its initial construction, or retrofitted in during renovation. Therefore, a basic understanding of construction techniques, the construction process, and certain important construction-related skills are necessary. Every modern security manager, for example, must be able to read blueprints and specifications, and should have a good sound grasp of how they apply to the corporate security program. Know and understand the steps in the construction process, and have a thorough understanding of the company's procurement requirements, during construction and under normal day to day operating conditions.

Probably most important of all is the ability to adapt technology to your specific situation. Say, for example, that you become Director of Security for a major art museum, responsible for the protection of a billion dollars in irreplaceable art. Not only must you keep more assets on hand than any bank in your city, but you also must hang these assets on the walls for all to see and approach, rather than store them safely in a vault. You must protect your collection, handicapped by a set of "rules" that apply to work in museums. These rules, among other things, say that security cannot be too visible; detectors must not be too obtrusive; you may not touch the pictures in any way with sensors or wires; you may not place anything in front of the picture such as glass or protective glazing as this will interfere with the ability to see the fine brush strokes. You will find that few companies make a product specifically designed to help you overcome the limitations placed on you in the field of museum security. So you have to improvise. With your knowledge and skill in the area of security technology, you adapt equipment made for one task to the unique task required of you. That's what sets you apart from others. That's what makes you an asset to your employer.

Your ability to excel in a technologically changing world will depend upon your ability to keep pace with the security technology. Know

the trends. Know how new technology is being applied to solve current problems. Your ability to foresee the changes in technology will enable you to make wise business decisions for your employer. Why buy old technology when you can buy technology that is on the leading edge. But how will you know, if you don't keep pace?

Learn how to identify trends. CCTV cameras get smaller and computers get smarter. It seems like only yesterday that we were all impressed that alarms no longer had to be annunciated by a blinking light, but instead printed out on a Teletype printer. Then everyone began to build proprietary, private label central processors to analyze alarm data and display it on a computer monitor. But these were expensive and out of reach for many of us. I remember telling everyone to buy computer-based systems that utilized IBM PC's to process incoming data. Why buy a proprietary computer that could be repaired by only one vendor when you could buy a computer than could be repaired at any local computer store? People thought I was crazy! I remember telling a product manufacturer how nice it would be to have a watch patrol system that used a hand-held reader to scan universal product code stickers. Presto! Now they are old hat! Then came color graphics on alarm systems, touch command screens, and cameras so small they can be concealed just about anywhere. Today, cellular phone technology offers alternate alarm signal transmission means, but I'm sure that by tomorrow, we'll be sending signals directly to the central station via satellite using a more "modern" means. When the technology is ready, I'll be ready to use it. If you plan to get to the top, you will have to be ready, too.

Prepare for your career in security by studying basic electronics and computer technology. You don't have to be a computer programmer to be successful. Your needs will require that you understand computers and know how to adapt existing applications programs. A basic course in mechanical engineering wouldn't hurt, either. But concentrate your formal education in the areas of business management, unless your school offers a specific curriculum in alarm system or similar technologies. Learn how to read a company balance sheet and annual report. Know how to do a budget. Above all, know how to write a good memo and lead a meeting in an articulate and professional manner. Without these skills, you'll be the potted plant, the "Lead Guard," whose security department is run by others!

The security industry offers a variety of highly specialized programs for learning technology. The National Alarm Association of America offers a 12 videotape course--everything you ever needed to know about alarm systems, CCTV technology, and similar systems, as well as the industry standards pertaining to them. Other programs are available from other professional sources, and seminar programs abound at trade shows and through the trade associations.

Finally, the security professional and the student of security management can fall back on the time tested "internship." Too few internships are offered today because employees and students expect to be compensated for their time as though they had technical skills to offer. If more students understood that an internship offers them an education that money cannot buy, they would jump at any opportunity to work for a locksmith or alarm installer, or to learn the ropes as an intern in a modern security department office in an industry they have targeted for their career. There is no better training than "doing!" If I had to learn technical security today, I'd do it differently. Rather than working my way through college in a factory earning minimum wage, I'd volunteer, if necessary, to spend my summers working with a locksmith, an alarm installer, and a successful security consultant.

Too many security managers and students of the profession never learn that it is not up to their teacher to teach them, it is up to them to learn from their teachers. The best way to learn about security technology is to read everything that is written and ask how it applies to their specific field. Grasp the basic concept of how security technology works, and everything else falls into place.