OPPORTUNITIES IN ACCESS CONTROL

By Isac Tabib

Oxford dictionary defines the word opportunity as "a set of circumstances that makes it possible to do something…" successfully. I added the word "successfully." In our business, we look for opportunities that help company growth, increase our customer base, improve the bottom line and build a company that makes us proud.

This combination will allow, at some point, retirement, with the knowledge that what we have invested our lives in—the long hours, time away from our kids, the financial risks—was for the good of our family, employees and customers. Easier said than done, for sure. It seems a lot needs to come together for opportunities to be realized and translated into success.

Security systems comprised of burglar alarms, closed circuit TV (CCTV), access control and others are all around us. There is hardly a nearby structure that does not have, or need, some type of security system, each of which provide us an opportunity to be involved.

In last month's *Doors + Hardware*, I wrote an article entitled *The Case for Access Control*, where I mentioned that I have been in the electronics security industry for many years. We grew our company to a multi-million dollar highly successful organization. Among the many projects we installed were thousands of access control doors. Each one of those doors needed an electrified locking mechanism. All of these were installed by qualified locksmiths, who for the most part acted as subcontractors. Each played a small part—installation of the electrified door lock—while simultaneously, losing the opportunity to play a much bigger role in further involvement from installation/service (think RMR) of the total security system being installed.

So, why are most locksmiths 'willingly' giving up the bigger opportunity, and instead playing a secondary role? The answer includes numerous variables. In this article, we will address two variables necessary for achieving a larger role in these opportunities and their success:

1) technical skills

2) solid product offerings

Technical Skills

You wouldn't take apart your automobile engine without the skills and knowledge of how it works so that you can successfully reassemble it in good running order. Possessing that knowledge and required technical skill sets makes you powerful. The quotation we've all heard—"knowledge is power"—is often attributed to Francis Bacon, in his Meditationes Sacrae (1597).

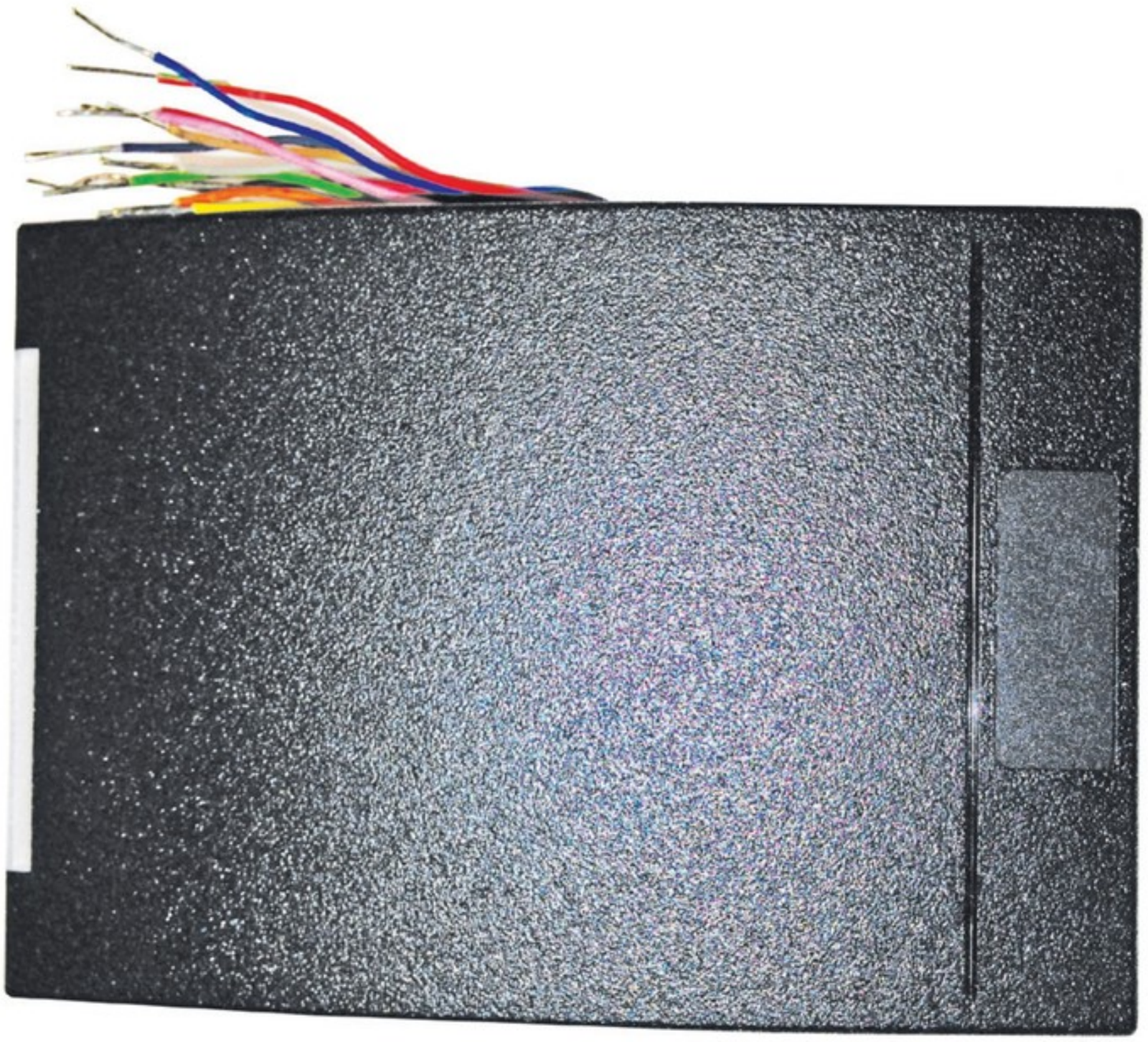
The concept of the quote is simple: the more you know, the more powerful you become. Hence, the more you know about access control, the more powerful and successful you can become in this lucrative business. Obviously, there is a lot to know, so we will handle one topic at a time while sharing my experiences. I hope that over time these articles will convey best practices to consider and follow and help you to become more knowledgeable and successful on your own.

The Access Control Door: The 4 Key Elements

Some of you may have a good understanding of access control, from the door hardware to the functionality of each of four key door elements:

1) **Card Reader (CR)**
2) **Door Status Monitor (DSM)**
3) **Request to Exit (RTE/REX)**
4) **A proper Electrified Lock (EL)**

Some of you may have working knowledge and might be a little fuzzy on answers to "how to" and "why," while for others, this may be the first time you're thinking about expanding your opportunity circle. Let's do a quick recap of a typical access control door and what I call the four key elements involved:



1) Card Reader

You are likely familiar with the ubiquitous proximity reader. Most look the same but, don't necessarily function in the same manner. Some are 'read only,' while others are 'read/write'—meaning additional data is stored and can then be 'written' onto the PVC cards presented.

Consider that the PVC proximity card you hold in front of the reader has a tiny ID microchip but does not have a built-in battery. Where is the power for the chip coming from? In a very simplistic way, the wall mounted card reader has a built-in coil that plays dual roles. Half the time the coil in the reader is powered and thus generating a magnetic field, while the other half of the time, the coil is behaving as a large antenna receiving the faint "bits" transmitted by the PVC card.

In addition to the microchip, the PVC card has a built-in coil and a capacitor. When presented within the magnetic field of the reader, the coil within the card generates a minute amount of electricity that is stored on the capacitor and powers up the chip. The chip then 'wakes up,' transmits its ID to the reader, and so on. This process takes place thousands of times per second.

The most common reader is a 'read only.' It is simple to install, very flexible, and requires 12VDC power (red/black wires, typical) to operate. It has a tri-color (red/green/yellow) LED, (brown/orange wires, typical). LED color patterns depend on the controller's type and wiring. The LED indicates certain door/read statuses such as door secured, door in alarm, door held open, access granted, access denied; and more.

A yellow 'beeper' wire (yellow color, typical) provides additional audible clues to supplement the various LED indications. The most common communication protocol between the reader and the controller is Wiegand. The Wiegand communication format requires just two conductors known as "Data 0" (green lead) and "Data 1" (white lead). Wiegand is a very reliable communication form with suggested no more than 500 feet maximum distance from the controller panel.

As mentioned, the faint card Binary signal (0/1) ID code is captured by the wall mounted proximity reader, the serial Binary stream is then transmitted via the DATA0/DATA1 leads to the controller. The controller then parses the data, matches it to a specific user, and validates the user against some 20 or so parameters such as who are you, what door you're at, time, date, is the card flagged as lost/stolen, any special instructions when this card shows up, and so much more. We will cover the controller's functionality in future articles.

It should also be noted that the Wiegand format is easily compromised, posing a greater system vulnerability. To overcome these shortcomings, newer generation of RS-485 serial readers, adhering to a universal (OSDP) protocol, are becoming more acceptable.

2) Door Status Monitor (DSM)

This is a simple magnetic reed switch installed on the door frame with a mating magnet mounted on the swinging/active door. The DSM is then wired, either in a supervised or non-supervised mode, to the controller. Since the use of the DSM is not mandatory, the card reader and electrified locks will function without it. For this reason, I find that many installers, both security integrators and locksmiths, choose not to install it. As mentioned, the card reader door

will function without the DSM. The questions then becomes, why use it at all?

As you might imagine, there are some really good reasons to use the DSM rather than leave it off. Let's look at a few examples:

Relock

When the controller grants access to a valid card holder, it will do so for a preprogrammed amount of time. Most manufacturers default the 'unlock time' for eight seconds. This is apparently enough time for an average person to, after presenting a card, pick up a box or similar (if needed), pull or turn the door handle open and go through the door. Doors that accommodate disabled persons typically require much more time—approximately 30 seconds—to complete the same transactions and move through the door.

In either case, during that time, the door is unlocked. Both eight seconds and 30 seconds are considered to be enough time for a "trailing person" to follow the valid card holder and enter the premise without authorization; again, the door is unlocked.

While testing these kinds of scenarios, I have gained entry to many doors and sites by simply trailing an authorized card holder. When a DSM is in use, following a valid card presentation, the door controller 'knows' or recognizes that the access door was opened and subsequently closed. After the door closes, the DSM signals the controller that the door is now closed, and the controller then 'relocks' and secures the door thus preventing a trailing person from entering the premise freely.

Door Held Open

As you might imagine, for various reasons following a valid transaction, Users don't verify that the door has locked behind them, that the door was inadvertently or perhaps deliberately, left open thus compromising security. During a recent site inspection, I was able to gain access to an important building via a door that was held open by an 8" rock someone deliberately left at the door. When using a DSM, the security system is notified of "door held open" violations, so that they can be addressed.

Door Forced Open

Similar to the door held open condition, we can also get an alarm signal if the door has been forced open from the unsecured side. Interesting to know, when using a card reader to enable entry from the unsecured side, after presenting the card to open the door, while pulling the door open, the DSM is triggered, which can cause an alarm condition. There is no reason to worry. The door controller automatically silences the "door forced open" alarm upon a valid entry.

Please note that the above features and notifications can only take place if a DSM is used. For this reason, plan on doing so as a best practice.

When describing the DSM, I mentioned the term "supervised." We will cover that feature in the future. Keep in mind that a good access control system would also like to know if someone has cut or shorted (compromised) the wire leading to the DSM. This is easily achieved via the installation of one, or two, End of Line (EOL) (inexpensive) resistors.

3) Request to Exit (REX/RTE)

From the above, we know that it is highly beneficial to use a DSM on every access control door. When in use, during exit and while pushing the door to open, a "door forced open" alarm is generated. This is an undesirable byproduct of the use of the DSM.

This issue is remedied through the use of an REX/RTE device. These devices come in a variety of shapes and configurations, however, they all achieve the same purpose—to signal the door controller before the door is opened from the secured side, that the next transaction (door open) is legitimate and that the door forced open alarm is suppressed.

Some RTE/REX devices are Passive Infra-Red (PIR/heat) motion sensors; others use ultrasonic detection method, while other REX switches are

simply built into the locking hardware. When ordering electrified locking hardware, as locksmiths, you are all familiar with the "REX Option."

In most cases, the REX has only one purpose: to suppress the door forced open alarm when exiting the secured space. When using a magnetic lock, as the electrified locking device, the REX is also used to unlock the door. Finer details regarding the use of "maglocks" will be discussed in a subsequent article. For now, think of maglocks for use only in the situation where there are glass doors.

4) Electrified Locks (EL)

These are available in what seem to be countless forms. You are most qualified to select the proper EL for the job. Do consider door/frame types, use, and required life safety codes, etc.

The Products: Adding Value for our Customers…

As mentioned, there are many pieces to the "success" puzzle. In the first paragraph, I mentioned the need for technical skills and having a solid product offering. In speaking with several locksmiths, I asked why they are not taking advantage of the opportunities to provide the entire access control system. I got almost the same answer from everyone I spoke with: it is complicated to install. I understand that. It is not that easy to become both a security expert and an IT person overnight.

"I've tried to install access control, but find it very difficult to achieve successfully," says Micha Snider of J&J Security in Long Island NY. "I know the basics [i.e. the four key door elements] but, the installation process of the software is complex, especially when it gets to the IP configuration and connecting the computer," he adds, "We even experimented with installing wireless locks but, found them to be even more difficult to install and complex to configure, as they need to connect to an access control system headend software which we do not manage."

As a security integrator for many years, we realized early on that we had to build an IT department to enable us the capacity to handle the technical issues described by Micha Snider and others. Most locksmith organizations do not have such network-centric resources available to them, forcing them to shop for easy to install systems they purchase through their lock hardware distributors.

"We get calls from various locksmiths, many of whom are pretty smart, asking if we have something 'simple and easy' to sell," says Eric Hagee of Accredited Lock in Secaucus N.J. "To be honest, we carry little variety in this regard, since we pride ourselves in providing support for what we sell."

"Tech support is very time consuming as well," adds Hagee. "Many manufacturers call asking us to sell their wares, however, we find that they don't offer anything different or new, that may be easier to install or, will minimize the number of support calls we receive. So, we stay with the lines we already sell. Having products that are simpler and easier to install will give us and the industry a much-needed boost. Today, everything is about price. To grow, we need to add value to our customers and their customers."

We understand this very well, as selling locks at reasonable and needed profit margins is becoming more difficult. There is a need to "de-commoditize" our industry. Adding value is the solution. You cannot go to Amazon and buy "value."

In spending time discussing current access control products offerings available to the locksmith industry today, I agree that they leave much to be desired. The opportunity to grow is knocking on our door. Acquiring the necessary skills and knowledge is a matter of commitment and investment. It seems this will only take place after there are good products available that are also easy to install and simple to program. In this regard, stay tuned as I am aware of a couple of companies that are trying to develop hardware controllers that are based on the "plug and play" concept.

ISAC TABIB is acting Vice President of Technology at DeltrexUSA. He has extensive experience is the design and construction of Integrated Security Systems and was a partner at Antar-Com Inc. Email him at isac@ifly51.com.