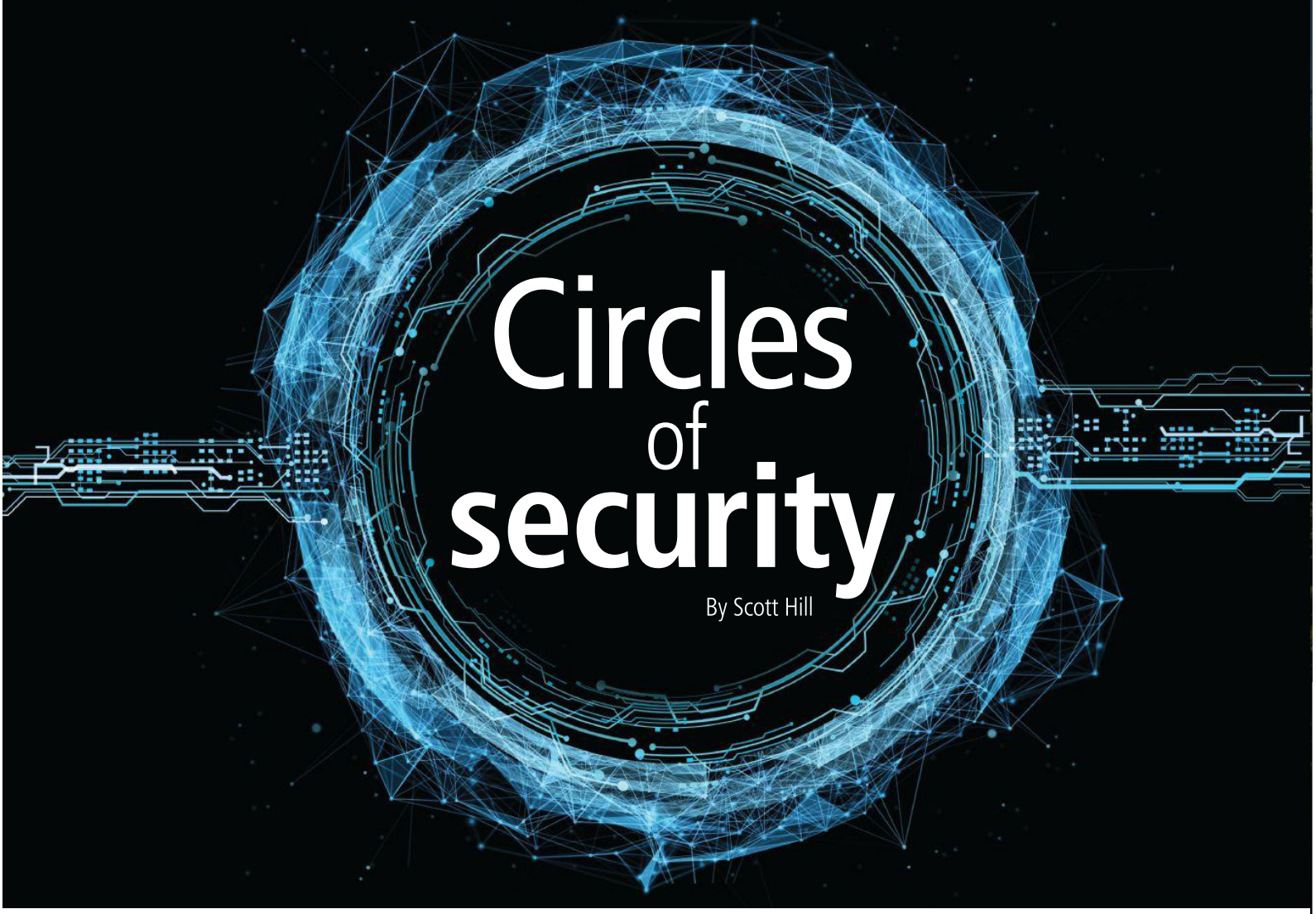

Circles of security

By Scott Hill

A layered approach that encourages back-ups, redundancy and multi-factor authentication helps keep assets safe

As technology and knowledge advance, clients are expecting more and more from their security installers and certified dealers.

Part of that reliance stems from the fact that they are looking to their security providers to stay current on security trends and be familiar with recognized security theory/principles. The security dealer who is able to present his/her security recommendations in a cognizant and professional manner, referencing established security principles, is bound to stand out from the masses.

One of the Security Principles that security providers would be advised to implement into their proposals/recommendations is that of Layered Protection.

Layered Protection or Defence in Depth is a security concept where assets are protected by rings of security measures. In the center of the rings is the protected or critical asset. As you progress from the outer to the sequential inner rings, at each layer, the security measures get more stringent. The reasoning behind this concept is illustrated as follows.

Although the critical or protected asset might be secured behind a locked door, if the access device (key, fob card, etc.) key is lost, stolen, or copied, then anyone in possession of said device would have unlimited access to the asset. Proper security design builds in safety measures and security redundancies/contingencies to ensure that any critical asset is not protected by a single security source. In layman's terms, security professionals should avoid "putting all their eggs in one basket."

> "Proper security design builds in redundancies/contigencies to ensure any critical asset is not protected by a single security source."

There are multiple advantages that will be realized by an installer/dealer when applying this concept to their proposals and quotes. A prime advantage is that, by showing a thorough understanding of physical facility security concepts, their clients will have more confidence in their recommendations and proposals. By doing this, they are positioning themselves to be regarded as an expert in their field, which will give credibility for all future transactions and ensure repeat business.

A second advantage to implementing defence in depth approach to security proposals is the ability and need to include contingencies/redundancies into a security plan. We can show this advantage by the following example.

A client has commissioned an access control system to protect their facility. A fob system is proposed and accepted. All exterior doors are protected (outer perimeter) with a reader that would require a fob to access the protected area. A reader is also put on the office door that contains the physical protection system (computer) which is running the required software for the access control system. The access level required to access this office would be set so that only administrators' fobs would allow access to the room. But what happens if the fob is copied, stolen or lost?

Access control systems are put in place to detect, delay or deter potential intruders if they attempt to access the protected area. Control to a building

A biometric measure, in addition to a physical fob and/or a password can help provide additional layers of security for high-value assets

can be managed by one of three (or a combination) processes. Access can be granted through something you have (key, fob, etc.), something you know (access code, password, etc.) or something you are (fingerprint, retinal scan, voice print, etc.). The stricter the security requirements are for the facility, the more controls and combinations are put in place.

Our previous example is an office with the critical equipment (asset) that requires protecting. Establishing that a single security solution (fob reader) is not sufficient to protect their area, a complete security recommendation would include (at least) one additional security measure to ensure that this asset is properly protected.

As demonstrated, in this example, we have already implemented a security measure that deals with "something they have" — a fob will allow access through the office door. As our earlier scenario questioned — what if the fob is in unfriendly hands, how do we still protect the office? The answer would be with a second security measure — in our example, something only an authorized person would know — like a numeric code.

When citing the Layered Security concept in their proposal or security design, the dealer and/or installer will propose (sometimes as an option, sometimes as a recommendation) that an additional security measure be added to the security design. In this case, something simple like door contact with a numeric keypad inside the protected area. Once the door is opened, the person that is entering the critical area will have a predetermined time to enter a numeric password (specific to each individual) which will terminate an alarm. If no (or the wrong) code is entered, the alarm is sounded. This alarm may be monitored so that an appropriate response (police or security personnel) can be dispatched to attended the site and deal with any intrusion. In our example, the fob system would be listed as the primary security measure and the door contact/keypad would be the secondary security measure.

The secondary measure can be a monitored camera, motion sensors, pressure mat, or any one of many intrusion detection systems (IDS). What matters most is that the two systems integrate with each other and protect the critical asset in a different, but harmonious manner.

Security installers and dealers seeking to increase their usefulness to their valued clients, will look to implement the Layered Security concept. First and foremost, it will better protect their client's property. An additional benefit is that it will raise the client's perception of their professionalism and their organizational commitment to providing viable security solutions. A final advantage will be the increased sales for the equipment that will secure their protected or critical asset. This is truly a win-win proposition for the client (who is properly protected) and the dealer who can ensure that they are selling/installing sufficient, proper, and enough equipment to exceed their client's expectations. SPT

Scott Hill of 3D Security Services is a Registered Condominium Manager (RCM) with the Accredited Condominium Managers of Ontario, a Physical Security Professional (PSP) with ASIS and a Certified Project Manager (CSPM) with the Security Industry Association.