3 Trends in PERIMETER SECURITY

Tightening down that initial doorway to your facility — perimeter security — can go a long way to keeping the people and products inside safe.

New dangers and improving technologies are bringing about changes to perimeter security.

By Tim Scally, *SDM* Associate Editor

End users are expecting more trust at the perimeter, and with improving technologies that are able to pull together video, analytics, access control and wireless communication, companies know that individuals are at the perimeter sooner and who those individuals are as they continue closer to a facility. This allows end users to grant access to trusted individuals and alerts them of possible threats, helping them to tighten their perimeter security.

Perimeter security is getting better as people rethink its uses and possibilities. Here are three trends that are taking hold in perimeter security today:

MORE FORTIFIED PERIMETERS

Many companies are looking to upgrade their perimeter security, and the good news is they have quite a few options for doing so. One way a customer can upgrade their security is by switching out older, single-factor readers to multi-factor readers. Often this involves biometrics.

"In general what we're going to see a lot more of is biometrics because of the uniqueness of it," says Craig Wilson, marketing and public relations manager for the Americas, Nedap Identification Systems, Branson, Mo. "The lack of a need to distribute the credentials because, obviously it is what the person is, and you don't have to remember a passcode — we do recognize that is the direction security seems to be going."

Another aspect of a more secure perimeter is the increased distance of long-range readers. As the credential moves towards mobile devices, says Brent Mahoney, enterprise solutions architect for G4S Secure Integration, Omaha. Neb., "[with] the advent of Bluetooth Low Energy as a credential, and even the app itself over cellular as a credential, more users are expecting a long-range experience from these devices instead."

Wilson says he sees virtual credentials as a huge trend not only because of the ubiquity of smartphones and the convenience of distributing credentials digitally, but because of the tendency people have to bring their phones everywhere. "People tend not to leave their phones," Wilson says. "You're less likely to depart your house without your phone than perhaps your keycard. So again, you get a better compliance level with added convenience and the ability to instantaneously revoke or distribute cards."

Some companies are pulling readers at the perim-

PHOTO COURTESY OF NEDAP IDENTIFICATION SYSTEMS

Scott Lindley of Farpointe Data says hybrid perimeter security systems that might not recognize a license plate but do recognize the access card, can alert a guard to see if he recognizes that person, who might just be driving a borrowed car.

eter and going to a longer-range reader — eliminating the threat of having a reader that is visible on the outside, says Scott Lindley, general manager, Farpointe Data, Sunnyvale, Calif. “Instead, they are going to a long-range transmitter technology, a long-range card technology, a long-range mobile technology where the reader is actually on the inside of the building under lock and key. It is protected from hackers and other bad actors.”

Convenience plays a large part in solutions working together. Convenience in perimeter security and access control isn’t important just for the sake of ease of use, but because it equates to increased compliance. “People tend to work around things that are inconvenient,” Wilson says. “People prop open doors if it’s troublesome to get in, or they disconnect equipment and things like that. We found that if the stuff that we sell has a convenience factor as well as the security factor, they get the same control without having to inconvenience users.”

MULTIPLE SOLUTIONS

Another trend in perimeter security is a desire to use security equipment beyond just the security purpose. For example, Lindley says verticals such as healthcare are benefiting from the multi-application capability of contactless smart cards, particularly DESFire, EV1 cards or EV2 cards. “They basically incorporate AES-level encryption on the connection between the cards and the readers,” Lindley says. “It’s state-of-the-art tamper protection, and the healthcare facilities are looking to use these because it eliminates the need for onsite personnel to carry around cash.”

The cards themselves can be used for more than general access, he explains. They do provide secure access, but they also can be used for paying for food at the cafeteria, as a record-keeping system for drug distribution, for logical access — logging onto computers that maybe contain HIPPA-protected

When Seconds Count

The headlines cannot be ignored, and every time there is another active shooter situation, such as the shooting at the YouTube headquarters April 3, 2018, the questions are raised about how such a shooting could have been prevented. These situations serve to highlight the importance of hardening perimeter security. Craig Wilson at Nedap Identification Systems calls perimeter security a facility’s initial doorway or access point.

“The closer in that [initial doorway] gets,” Wilson says, “the closer your threat gets to you before you can do the ‘deter, delay, detect scenario’ that security is designed to do.”

Having a robust perimeter security solution buys a facility time and protects the inner facility from a breach sooner. “If you’ve got a facility that needs that kind of security from an intentional threat, or even an accidental one,” Wilson says, “it just comes down to risk exposure and how much you’re willing to tolerate and how much you want to trade off against equipment installation and upkeep costs and things like that.”

Michael Dorrington at Electric Guard Dog says criminals will always look to strike a non-hardened site first. “Why bother with a potential problem or encounter with the police?” he asks. “Instead hit a soft target that will allow you to take your time. Security perimeter systems alert the site owner and police of intruders.”

However, if the bad guys want what you have, Dorrington says, or in the case of an active shooter who is targeting a specific facility, such as a former workplace, they will find a way in. “It’s up to the property owner to deter criminals from entering a site,” he says.

Ultimately, Wison says, you don’t secure at your own risk. “There’s a liability associated with that; if you’ve got a facility that has some sort of risk to the public or something desirable in it and you don’t secure it, you expose yourself to lawsuits or theft or loss of life.”

Often, perimeter security can go a long way to keeping the people and products inside safe.

information about patients.

Applying this trend specifically to perimeter security, Wilson says there are technologies that will identify not just who is driving a vehicle, but also the chain of custody. "We've had vehicles that use the technology not for security but they use it for time and maintenance. So when the vehicle goes into the maintenance shed, the time it is worked on and when it leaves — they can use that for their operational facility as well. It's just a broader use of the technology, which I feel is good for everybody concerned, because those things have been siloed in the past."

PHOTO COURTESY OF NEDAP IDENTIFICATION SYSTEMS

Customers are finding broader uses for perimeter security technologies. Craig Wilson of Nedap Identification Systems says they've had vehicles use the technology for keeping track of a vehicle's time and maintenance.

Michael Dorrington, vice president of sales and marketing, Electric Guard Dog, Columbia, S.C., adds, "The Internet provides an always-on, real-time connection to the world. For example, at Electric Guard Dog, our building access cards give us the ability to make payments at local eateries and retail stores. It provides a series of benefits that are available to the University of South Carolina's faculty and students."

SHIFT TO UNMANNED SECURITY

Another trend in perimeter security is a tendency to lean more on technology than on humans. While humans still play an irreplaceable role in perimeter technology, particularly in more high-security applications that require human decision-making, using technology as a response force is a huge growth industry, Mahoney says. "From automated voice response to drones to robots, the security trade really sees this as part of the future in our SOC designs. Cost has also come down on many technologies, taking what used to be available for only the very largest budgets and most critical projects and making it affordable."

In fact, Dorrington says cost and effectiveness are forcing facilities to look to unmanned options. "Analytics are becoming more cost effective," he says. "These systems are getting smarter, allowing for traps to be set that alert the user of system trouble. System analytics is a trending solution that is making perimeter security more efficient."

Dorrington also emphasizes the importance of updating infrastructure for unmanned applications: "Solar power, wireless integration and narrow bandwidth are musts in security today."

Lindley says that while in the past someone had to be sitting at a desk watching the video feed, perimeter systems now can have triggers. "The video itself can be looking at license plates; it can be looking to, 'Hey, is that a standard car we expected? Is this a standard card number we expected?' and then it grants access. It's fully automated."

He says there could be a hybrid system in which if it's a different license plate but they recognize the card, then maybe a guard needs to take a look and see if he recognizes that person. "Maybe they are just driving a rental car, for example," Lindley explains.

In some instances of high security, however, Wilson cautions that good old-fashioned manned security remains a necessity. "There are a lot of things that a person can see, detect and understand that technology just can't do at this point."

But even in these instances, the relationship between humans and technology in perimeter security is becoming symbiotic in some ways, as evidenced by instances in which technology is required to override human error. "We've done several jobs at casinos where they use our technology to tag the casino keys so that the manager doesn't accidentally leave with them," Wilson describes. In this case, the casino's policy had forced it to terminate some forgetful but otherwise good employees. "They use it as an alerting system that basically just says, 'Hey, don't forget you still have your keys; don't leave the building,' as they're starting to exit."

But as long as a human is harder to hack than a machine, there will always have to be a human element in high-security situations as perimeters continue to facilitate more unmanned technology.

Ultimately, learning that someone is at the perimeter sooner, and who that person is, is becoming easier and more convenient. The biggest factor, however — trust — hasn't changed. Trust in technology, trust in employees and trust in the integrator designing the system must all be factored in to any perimeter security solution. The good news is the industry is trending toward being better suited to facilitate that trust. ■

MORE ONLINE

For more on perimeter security, visit *SDM*'s website for the following articles:

"Perimeter Security Becomes a Main Focus"
www.SDMmag.com/perimeter-becomes-focus

"A Dozen Tips for Tighter Perimeter Security"
www.SDMmag.com/12-tips-tighter-perimeter