VANDERBILT

News

***This article originally appeared in A&S Magazine. Read the full post here.*

Dual authentication is an option in any mixed technology environment, but the technology applied should be determined by the individual use case, according to Martens, Futurist at Allegion. In many circumstances, a smartphone is already validating the identity of the user prior to presenting a smart credential to a reader.

Others vary in their opinions. Daniel McVeagh, Senior Product Manager at Gallagher explained that while not a must, adopting a multi-factor identification solution in a combined logical and physical access system is advantageous from a security standpoint, with lost credentials becoming less of a security vulnerability.

“Including a biometric identifier in the solution solves the problem of employees sharing the access credentials or passwords with other employees, ensuring the person at the door or logging into the network is, in fact, present,” McVeagh said. “As issuance of identity

credentials to mobile phones becomes more prevalent in access control systems, we expect these mobile credentials, along with the phone's native biometric authentication capabilities, will be used more frequently as authentication means at both door readers and for accessing logical assets."

Julian Lovelock, VP of Strategic Innovation at HID Global, gave further inputs on the matter, adding that multi-layered security strategies will continue to be critical for protecting systems and assets as well as the user identities that facilitate authentication.

"Biometrics will play an increasingly important role," Lovelock said. "As the only available way to bind a myriad of digital and physical credentials to our one true identity, biometrics is helping to eliminate digital identity theft in today's increasingly complex and vulnerable digital environment. Watch for solutions that combine biometric liveness detection with other security layers to greatly enhance our digital security while also ensuring that stolen biometric data is insufficient -- and therefore useless – for the fraudulent use of legitimate identities. And yes, users should have a wide variety of options for securely carrying their trusted IDs, from phones to wearables to fitness and health devices. The next frontier of mobile choices and solutions is the ability to carry driver licenses, passports, social security cards and other citizen IDs on mobile phones, as well."

Then there are others who stress the part that multifactor identifications are not a must in this form of integration. In the view of Mike Sussman, Technical Director at TDSi, at the end of the day, the type of credential used for both is dependent upon the risk of the data and systems you are trying to protect. This can be as simple as a password for logical access and a proximity card for physical access through to RSA keys and biometrics.

"When considering multimodal, thought should carefully be given to the user base and if using mobile devices then the type of device to ensure that any method will work on all mobile operating systems," Sussman said. "Logical can utilize everything from a simple PIN to two-factor authentication using codes."

The access control industry is seeing a significant shift in card access readers toward multi-identification in an effort to safeguard identities and critical assets, according to Mitchell Kane, President of Vanderbilt Industries.

“So many times, a key card is lost, leaving an organization vulnerable without multiple steps to determine whether the user is in fact allowed access to a specific door or building,” Kane said. “This shift to multi-identification – whether it’s through biometrics such as an iris or fingerprint scan, or even a personal passcode that must be entered – safeguards a person’s identity by requiring multiple levels of access control. This approach is quickly becoming the next wave as enterprises look for new ways to protect critical data and assets from internal and external threats.