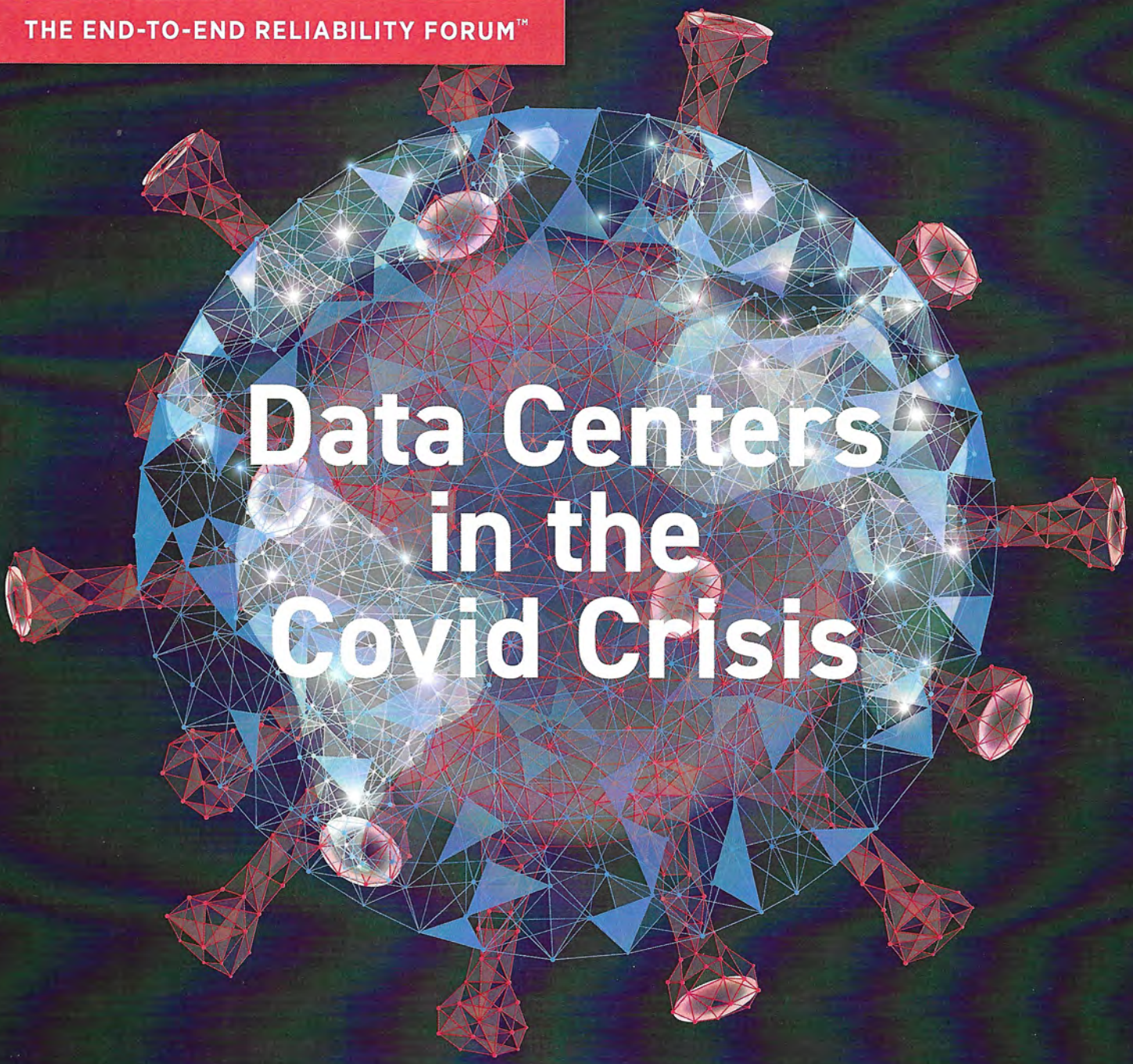
PUBLISHED BY 7X24 EXCHANGE INTERNATIONAL

7X24 Exchange® INTERNATIONAL

THE END-TO-END RELIABILITY FORUM™



Data Centers in the Covid Crisis

OUR NEW NORMAL

Data Centers Should look to Biometrics to Ensure the Safety of Employees as well as Facility Security

by Andrew Graham

Biometric access control is by no means a new concept for the data center industry. In fact, a significant number of data centers employ some form of biometrics in their facilities. While they haven't been the easiest technology to deploy, fingerprint readers coupled with passcodes or proximity cards, do a good job of authenticating the identity of your personnel. Ironically, what's keeping your data center safe is now endangering the health of your employees, vendors and clients.

TODAY'S NEW NORMAL

Fingerprinting at the DMV, airports, office buildings, ATMs, etc. was largely halted in response to COVID-19. As the country reopened, strict disinfecting protocols were introduced to sanitize touch-based access control technology like fingerprint and palm readers, touchscreens and keypads. But ongoing disinfection is a short-term solution. Disinfecting chemicals simply aren't suitable for long-term use on delicate surfaces and electronic equipment. But more importantly, hygiene concerns remain even with the strictest of protocols. The fact is that no one will ever want to touch publicly used access control equipment again. Period.

It's this insurmountable challenge that has essentially killed the market for public-use fingerprint sensors and palm vein hand readers. Industry analysts forecast in 2-3 years this technology will be completely replaced by touchless biometric solutions. They go on to say that multi-modal authentication technology will be increasingly deployed in public and commercial environments where security is just as critical as employee safety.

MULTI-BIOMETRIC AUTHENTICATION – YOU ARE THE KEY.

Biometric recognition provides a distinct association between an individual and a claimed identity. It is a unique natural measurable pattern that is nearly impossible to duplicate. Unlike a password that can be forgotten or a proximity card that can be lost or stolen, all forms of biometric authentication have the least probability of being tampered with.

However, nothing's perfect and that includes touch-based biometrics. Well before COVID-19, we were

aware of accuracy issues that happen when using a single method of touch-based biometric authentication. For example, the accuracy of a touch-based fingerprint can be affected by the pressure put on the device, as well as dirt on your hand or skin damage. A palm vein reader can be affected by swelling and contraction caused by temperature changes.

Additional accuracy issues can arise if you use only a single method of biometric authentication. When you scan your fingerprint, palm vein, face, etc., what's stored and analyzed is a measurement of various points of that biometric marker – not a detailed picture of yourself. If you want higher accuracy you should consider a multi-modal biometric system that utilizes many more points. Today's technology gives you the option of using any combination of four authentication markers – face, fingerprint, iris and palm vein – in a single reader unit.

Being touchless isn't the only way biometrics help ensure your employees' health. Real-time facial recognition can now occur in under 0.001 second. Iris identification can occur at much longer distances. The technology's ability to achieve near-instantaneous identification reduces congestion and lines at your facility's point of entry. Less congestion translates into fewer opportunities to spread viruses.

THIS ISN'T YOUR DAD'S BIOMETRIC TECHNOLOGY.

I'll be the first to say that the installation of biometric technology in the data center has historically been anything but fast and seamless. In addition to accuracy issues and slow processing speed, deployment usually meant ripping out the old and installing all new – new hardware, new software, and new processes. Nothing could be easily integrated, if it could be integrated at all. Often systems ended up being neglected, thereby creating bad data and security risks.

The integration capabilities of today's touchless biometric access solutions are vastly improved. Solutions are now compatible with, and can attach onto, any third-party system utilizing RFID, Wiegand, RS-485 and a web-based API. The enrollment process is also quick and easy – as fast as three seconds!

Better integration capabilities also mean you don't have to replace all forms of access control to protect against germs and ensure facility security. Pairing multi-biometric identification with RFID proximity cards, for example, reduces human touch points and provides the multiple factor authentication you need to be in compliance with HIPAA and FISMA standards.

TOMORROW'S NEW NORMAL

Thanks to COVID-19, we will never return to "business as usual." But there is a path forward. All the experts agree that touchless technology is here to stay. While touchless biometric authentication can replace all forms of access control throughout the data center, it doesn't have to right now. Your urgent need is to reduce points of contact between human hands and equipment. Touchless biometric access control solutions can easily replace touchscreens and keypads and work seamlessly with your existing touchless technology.

Andrew Graham is the Director of Data Center Solutions for Critical Environments Group. He can be reached at agraham@criticaleg.com.