Guidepost

DATA CENTERS – SECURING MORE WITH LESS, LESSONS FROM A PANDEMIC

In the weeks following the spread of COVID19, countries and businesses were abruptly forced into critical decisions relative to reducing or ceasing operations, defining essential operations and maneuvering multiple mandates. The resulting questions include, how are we going to do more with less and how can we ensure the safety of our people and the security of our business? Some had no choice. Emergency and primary healthcare are always essential while businesses directly serving the public such as delivery services, grocery stores, and drug stores are by default essential to maintain a healthy public.

By the end of March, regulated geographies impacted nearly half of the global population. Most workers moved to remote home offices and students switched to online learning. As people locked down, online traffic increased by over 70% and streaming services increased in volume by over 12%. Quietly the Cloud had become more than essential and the data centers that provide an actual physical home to Cloud and computing services were clearly, even if not designated, essential to our pandemic mode of operation. Industry leading data center operators faced key questions about how to continue operations, mitigate the risk of employees contracting COVID-19, and secure facilities with less.

How does your business continuity plan measure up?

The speed at which the virus moved across the globe caught many business experts off guard and a variety of business operations were caught on their heels working through outdated business continuity /disaster recovery plans – plans that did not properly account for a global pandemic nor the rerouting of all business operations to remote locations. Data centers, however, have spent the last decade fine-tuning how to ensure the required uptime of their facilities with remote monitoring, maintenance and operations. Data center operators implemented technologies to secure facilities, including improved access control to deter incursions and video capabilities to monitor critical operations such as air-cooling units, PDU's and backup power systems. Much like a consumer's phone or fitness watch, data center operators could ascertain issues with any number of systems remotely and in real time prior to the system or component failing. This ever-increasing advance in technology allowed data centers to quickly reduce on-site operational capabilities, augment staff scheduling, and determine which components of their business were essential to ensure unimpeded operation of their mission critical facilities. Business leaders can glean some valuable lessons

from the approach taken by data centers.

Ironically, the efficiency of operating and maintaining the mechanical components of a data center have improved as a result of the same digital technology in which they host. Securing these facilities during the pandemic has taken on an even greater level of urgency as staff was reduced and the public became more reliant on digital business being hosted within the walls of the largest data centers in the world. With operations minimized, some providers significantly reduced their internal operations and closed European operations to customers needing access to their sites. Many operators adjusted and reduced staffing globally. Some augmented internal operational guidelines for site access to include temperature scanning and pre-access screening visitor access to sites. Site security workers, already essential to maintaining both a secure and hospitable environment for data center customers, were now on the frontline of ensuring the facility would be secured from standard external threats and an unseen, highly contagious virus. Data centers would be forced to utilize all aspects of their enterprise access control and video solutions to accommodate for a variety of variables including a reduction in staffing, augmented site access requirements, and physical tours throughout the facility. While some eliminated customer access in Europe, most commercial data centers could not simply close their doors. Mitigating customer access could potentially disrupt critical services provided by a variety of companies and public sector entities. These mission critical tasks would lead to newly updated Standard Operating Procedures (SOP) to allow operators to properly manage their reduced and remote teams. Companies implemented temperature screening and site disinfection requirements with other data center operators across the globe evaluating solutions such as:

- Enterprise Voice Over Internet Protocol (VOIP) to allow for remote communication
- Video Analytics
- Thermal Imagery
- Facial Recognition
- Remote Global Security Operation Centers (GSOC) Capabilities
- Managed Concierge Services
- Virtual Credentials

Currently employed enterprise level systems allow for the management and operation of remote security, however, in some scenarios these capabilities fall short. For example, localized intercom communications, manual issuance of access credentials, and integrated visitor management platforms lack remote security options. In other cases, the highest level of securing access points within the data center itself became a flash point for viral concern (such as with the use of contact biometrics). Highly secured areas within the data center may require use of a card reader and fingerprint reader for dual authentication access. In January, this level of access was considered critical. In April, facial recognition and frictionless access control were the top priorities. Other emerging technologies, such as thermal screening require greater level of on-site personnel to operate effectively. Even with new technologies and a quick pivot by most in the industry, securing more with less was still a challenge — one that has evolved as the pandemic spread.

The post-COVID-19 Context

In my 25 plus years in the security industry, I have had the pleasure of designing, coordinating and implementing high level security systems for the data center environment. As security is a critical feature to the data center operator, most locations have been thoughtfully planned and designed for the highest level of security systems implementation. Local operational staff and supporting security team members are reliant on complex and integrated security solutions and security workflows that dovetails the technology and the operational management. Facilities have been located areas that are remote from central business traffic to better ensure a cost effective and more controlled environment, but with the proper level of accessibility to power and infrastructure. Buildings have been hardened with perimeter fencing, facility-wide video coverage and blast resistant materials, all deigned to protect against potential threats to the digital economy that drives most of our business today. However, in what seemed like a moment's notice, today's threat became one that was not only unseen but had the ability to mitigate the very systems and processes that have protected data centers. In many industries, the terms security and safety have now taken on a new context as organizations pivot to protect their people while remaining flexible to the changing global environment.

TERRY KING

Regional Director, EMEA/APAC

Terry K. King is an expert in the design, consultation, and implementation of electronic security solutions. He has more than 25 years of experience in both security consulting services and systems integration. Mr. King specializes in large, new construction commercial projects placing an emphasis on effective communication between critical stakeholders and all associated trades and partners. Further, he has significant experience in the development of design standards for electronic solutions in both commercial and public sectors, ranging a wide degree of vertical markets. In addition to his design and engineering experience, Mr. King has a significant background in the assessment and analysis of existing facilities, including security systems, operational security, and standard operating procedures. His expertise extends to the program/project management of large-scale implementation projects, and the administration of standardized systems.