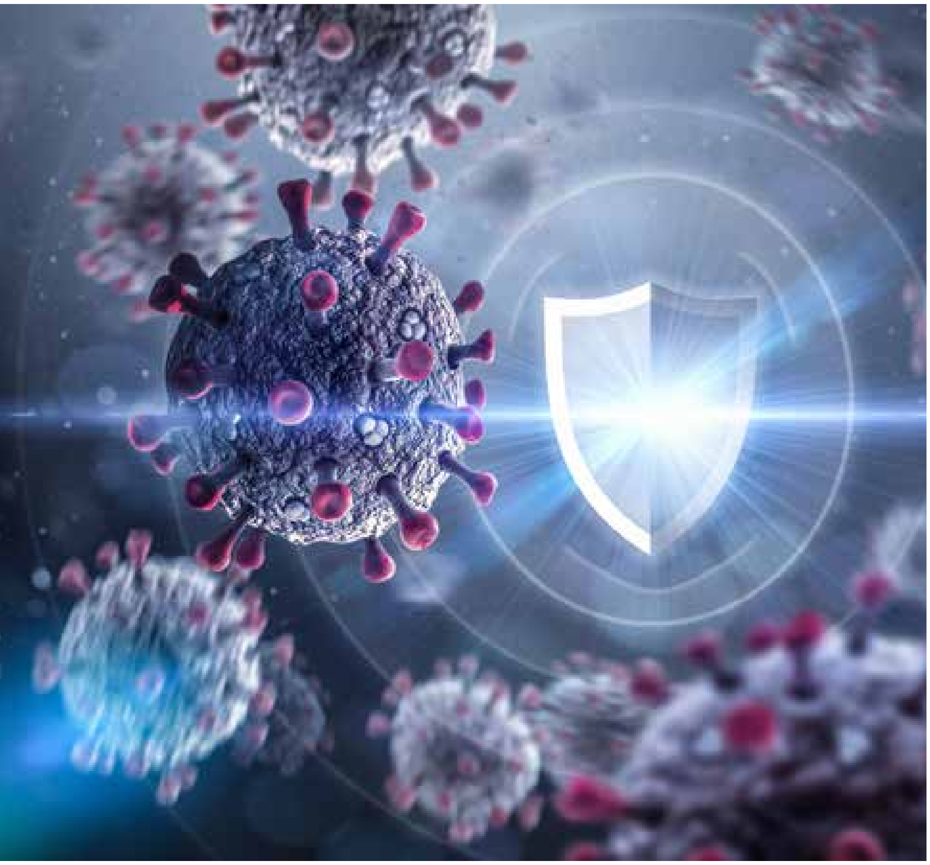
COVID-19's Impact on Facilities Cybersecurity

By David Handwork



"COVID-19 changes everything." Since early March 2020, this statement keeps popping up, morphing, and adapting to fit the context of each unique conversation. Indeed, with each advancing day of the 2020 crisis, all of us desire to transform the numerous unknowns of COVID into absolutes and assurances. Leaders of higher education institutions and facilities managers are deeply longing for fiscal certainties. Only time will reveal the realities of enrollments, on-campus housing occupancies, intercollegiate sports, the stability of foundations, federal and state funding, and other sources of institutional revenue. Facilities managers are not generally equipped for a new operations strategy with a future that is ambiguity rich and clarity poor. APPA's 2019 strategic plan, "Preparing for Every Future," is more relevant than ever, and is well poised to equip facilities professionals with tools, resources, and training.

Preparing for any post-COVID future requires a mindset of flexibility, adaptability, courage to take risks, and knowledge-based wisdom, to be able to develop and "sell" a malleable facilities management (FM) strategic operations plan to administration. The impact that FM has on student and staff recruitment is well understood. Equally understood is FM's impact on operations budget control, specifically related to capital planning, space management, and stewardship of energy, environmental sustainability, and campus assets. The temptation to heavily leverage the facilities operation budget for university budget reductions will be evident, but senior facilities officers (SFOs) should resist this temptation if at all possible. Even with an uncertain future, one predictable post-COVID outcome is the *increased expectation* of even more effective and efficient facilities operations.

Two available resources for facilities managers to address reduced budget expectations are 1) expanded use of automation and 2) emerging FM technology. Arguably the only purposes for utilizing automation and technology are addressing a solution to a problem and/or improving efficiencies. Applied facilities technology is not a panacea for operational budget cuts, yet it will create new efficiency opportunities and provide more cost-effective investments for automation and facilities informatics. Facilities managers should understand that proliferation of operations technology (OT) will create more cyber vulnerabilities with the continued propagation of the Internet of Things (IoT), networked systems, cloud-based software solutions, and evolving "work from home" strategies.

Effective cyber risk mitigation can become a reality for our institutions by embracing the following two principles:

Principle 1: A healthy SFO and CIO relationship. This is a primary principle for highly effective applied FM technology. Traditionally, SFOs and chief information officers (CIOs) have limited work engagement at best, primarily interfacing with departments on construction projects. That's unacceptable now and in the future. OT and IoT for typical and "smart" buildings require a higher level of FM and information technology services (ITS) departmental integration and interdependence for building operational effectiveness and security.

SFOs and CIOs need to view each other's departments as partners for achieving the institutional mission as well as supporting each other's departmental strategic initiatives. As a partner to FM, IT departments define and enforce cybersecurity for FM hardware and connected devices. Not engaging ITS can create challenges with OT and IoT deployments, especially when engagement occurs after the concept and planning phases. ITS can advise on industry and campus standards for connected devices. Registering these devices before connecting to the network is typically required for operations and security as well. Along with connected hardware and device standards, CIOs can also support facilities software platforms, especially if data is managed on-premises.

Regardless of reduced budgets, facilities managers and SFOs need to be ready to expand existing technology or deploy new technology. Otherwise, returns on investments can be delayed if cybersecurity standards are addressed postdeployment, or even negate technologies if OT/IoT devices cannot meet cybersecurity standards.

SFOs should work with CIOs and FM operations staff working from home—now and potentially regularly in the future. Remotely accessing energy management systems, work order systems, and other FM-centric software systems became a reality with COVID, something not generally considered prior to the crisis. Remote access, even with virtual private networks (VPNs) or other security measures in place, can create additional cyber vulnerabilities not only for FM systems, but for the whole campus.

The expansion of technologies and automation will continue to create more remote FM operations. For example, night shift custodial staff may work from home managing automated floor and restroom cleaning equipment, and landscape services may manage automated mowers. These systems are already in service today, not in some future world. These are the types of remotely managed capable technology that COVID will make cost affordable. But remote connectivity, even with low-bandwidth residential systems, will require support from ITS departments to be functionally effective and secure.

Principle 2: A healthy knowledge of facilities technology. SFOs and key FM leadership must become even more knowledgeable about emerging and viable facilities technology. Although ITS can support cybersecurity and data management, they are not facilities managers, and therefore completely inadequate to understand how applied FM technology enhances FM operations. COVID will change the value proposition of many applied technologies, including the emerging field of facilities informatics (applied facilities data science).

APPA membership engagement opportunities will certainly evolve to include more web-based connectivity and information-sharing events, such as the very successful APPA Town Halls that were recently held to share COVID response knowledge. Many institutions will struggle fiscally to justify or even pilot test technology strategies, while others are positioned to execute or expand their technology initiatives. APPA members should proactively share challenges and successes to ensure technology investments produce highly predictable, positive results.

COVID has certainly created significant and lasting challenges. But as APPA members, we are in this together. By collaborating and engaging with each other—member to member, SFO to CIO, peer to peer—we can leverage rewarding technology opportunities while keeping our campuses cybersecure.

David Handwork is assistant vice chancellor of facilities management at Arkansas State University, Jonesboro, AR, and APPA's Vice President for Information and Communications. He can be reached at *dhandwork@astate.edu.*