Guidepost

AFTER STANDING VACANT DURING THE PANDEMIC LOCKDOWN, IS YOUR OFFICE ENVIRONMENT SAFE FROM A PHYSICAL AND CYBERSECURITY PERSPECTIVE?

As the roll out of COVID-19 vaccines picks up steam, business leaders should begin considering remobilization and the physical return of employees to the workplace. Before opening your doors, however, it is important to consider where your security environment stands.

Before the pandemic lockdown, many businesses operated with robust physical security programs and cyber hardening measures that placed an emphasis on maintaining the safety and security of their people, and a focus on preventing outsider threats from penetrating critical network infrastructure and sabotaging intellectual property. While many of your pre-pandemic office and business operations environments remain, it may be risky to assume that the conditions left behind a year ago will be found in the same state. And will your current conditions meet the 'new' working environment your employees will expect?

Many business owners and operators acknowledge that change to the working environment must and will occur. To ensure that your workplace remains safe, you should consider and assess several important contributors to your security posture. These include environmental security, physical security, and cybersecurity.

Environmental Security

Examine what has changed about your business location in the past year. Has there been an uptick in crime since the pandemic hit? Consider the impact of crime on your business operation and the safety and security impact upon your business assets and people. Are there specific trends and patterns in crime activity, i.e., unauthorized entry, vagrants,

serious crime including aggravated assault, rape, and homicide? Consider how crime statistics, both existing and future forecast, may affect your security program and current mitigation plans. Do you need to update your security program policies and procedures to reflect the new environment of operation?

Physical Security

In terms of physical security, the factors to consider may include reassessing the security technology currently deployed. Do your systems still function in a manner that meets new operational needs? Is the pre-pandemic functionality of systems reflective of current and new operational needs? Are electronic security technology systems supported by back-up power measures and are they functioning as intended? Are there any compromises to the built environment that need to be remediated? Does the built environment path of travel for pedestrians flow in a manner that supports and maintains potential future social distancing needs? Is there seamless touchless entry and egress capability? Are there maintenance issues that need to be addressed that compromise your physical security program and are electronic security program updates current, have systems been maintained during the work from home period?

Cybersecurity

Cybersecurity measures to secure critical network infrastructure play just as an important a part of your security posture as business location and physical security measures. Cyber measures serve to prevent an often-silent breach to gain unauthorized access to protected data and intellectual property. Implementing measures and employee training to generate good cyber awareness and prevent against phishing, ransomware, malware, and other cyber-attacks should be considered. If your business did not consider or implement cybersecurity measures pre-pandemic, now is the time to address and correct the situation. The returning workforce lives in a world that thrives on the Internet of Things (IoT). Personal devices are a source of weakness and penetration when connected to your business networks. Implementing cyber measures to mitigate risk and maintain business continuity should be at the forefront of your return-to-work process.

With hope on the horizon for a return to some semblance of normalcy, the call to fully reopen has begun. Before opening the doors to your workforce, perform environmental, physical, and cybersecurity assessments. It may be prudent to engage an outside team of experts that is well-versed in performing such assessments, that can quickly identify areas that have or could be compromised and substantiate the risk and probability impact with solutions to mitigate risk and strengthen your organizational security programs.

NICK HEYWOOD

Associate Vice President

Nick Heywood is an experienced security consultant and project manager who excels at performing security and safety assessments and developing existing conditions observations into workable solutions that enhance a facility's security posture. Mr. Heywood has overseen projects in verticals including healthcare, corporate, detention and education.