LAYER SECURITY PRACTICES

TO CARE FOR YOUR EMPLOYEES

The active shooter attack in Parkland, Florida, was of course an atrocious act. Preventable? Possibly. Regardless, we must continue to improve what we do to both identify and act on developing situations before they hurt important lives around us, or become deadly.

Search "Defense in Depth" or "Layered Security" and the most common concepts that come up focus on cyber security. The mass shooting at a Broward County, Florida, school is a harsh reminder that the defense in depth concept also applies to physical security of our most precious resource – people. "Defense in depth" is a security phrase used to identify the practice of layering security measures and protocols for the greatest effect. Historically there is no single effective measure or protocol. It takes a well-designed layered approach shaped to identify and coordinate response to specific local possibilities to be effective. It all starts well beyond the facility fence line or parking lot.

The outer physical security layer focuses on understanding the local (or regional) environment and threat-scape as a whole, and specifically the people or groups comprising those threats. The environment may reside in a stable upscale community, a desolate and possibly crime-ridden industrial area, or an overseas project in a country grappling with social and economic discord. The process of securing your resources, your project, your employees, is the same – understand the local threats, those entities with a capability to do harm, and the capabilities they have at their disposal to inflict harm. Those threat-entities represent a risk to your people and must be fully assessed and countered.

An often missing component of layered security planning and implementation is to look inward. It is not enough to only identify the "external" threat. Have a critical eye toward identifying and understanding your organizations' vulnerabilities. Accepting and assessing those vulnerabilities is key to a successful plan. While leveraging your strengths is a great start, leaning only on those strengths is not typically effective in preventing a rupture in your security efforts. Be honest and thorough - your employees deserve a realistic vulnerability assessment, and an effective plan to reinforce those vulnerable areas. So you know where your vulnerabilities and resultant risk are, now what? Unless you have an unlimited budget (don't we wish!) you cannot afford to eliminate or even address all risks. But you can identify the primary risks such as those most likely or most dangerous to your business and employees. Time to conduct a formal risk assessment and engage your key personnel to make sure you are on the right course to effective incident prevention.

Finally, prevention. There must be a solid, tested plan to counter, to mitigate, identified risks to the best of your ability. This requires several layers of action from knowing your environment and monitoring changes in that environment, to identification and strengthening of increasingly "hardened" perimeters – the closer a threat comes to the business the harder it must be to inflict damage. These mitigation efforts may impinge on freedom of movement or personal privacy. They may create delays and may even create additional risk points to address. Work through those developments and most importantly coordinate with your local response resources like law enforcement, emergency medical services, and fire department to walk through your plan and make suggestions. It takes a continuous, collaborative effort to keep your employees safe.

There are numerous elements of each step in an effective physical or cyber defense in depth process. Partnering with a competent security organization to fully assess your situation and generate specific, effective security protocols that fit your employee and business security needs.

Arnie Tyler
MerLion Advisory Group, LLC
atyler@MerLionAdvisory.com