Security Leadership Solutions Executive Council

It's Not Too Late to Begin H1N1 Planning

In early September, the Harvard School of Public Health reported that the majority of U.S. businesses would have serious operational problems if the swine flu, H1N1, significantly affected their workforce. The announcement is based on the results of a summer survey of more than 1,000 businesses across the country spanning all sizes and industries, including critical infrastructure. The survey found that only one-third of businesses believe they could sustain their business without major problems if half their workforce were absent for two weeks, and only one-fifth believe they could avoid such problems if the pattern of absenteeism continued for one month.

By Rad Jones

The Centers for Disease Control (CDC www.cdc.gov) cannot accurately predict whether these levels of absenteeism will be likely, but they have made clear that businesses should prepare for that possibility.

DHS has been recommending that businesses large and small prepare, and while the Harvard study is evidence that many businesses have not done enough, it's never too late to start. Many security practitioners, however, are wondering what their role should be in this preparation. If your company has not yet developed a plan for dealing with H1N1 or if you have not been brought into the planning, here are some points to consider.

How to Plan

If your company already has an established crisis management team consisting of key company components for critical incident planning and response, you can build upon that framework to develop your contingency plans for H1N1.

If your company does not have an established crisis management team, pull one together now. Identify the key functions of your business, find out who is in charge of each, and get them together. Don't get hung up on titles; in a small or medium business, you may not have a director of security, a director of HR or a head of operations. But someone is a decision-maker in each of those areas, and that's the person who needs to be on the team. Discuss with these business leaders what makes the business run and how they could make up for it if any one of those crucial elements was handicapped by absenteeism. That's the start of your contingency plan.

Any H1N1 planning and response must also include input from local and state health departments and information from the CDC. Local and state contacts are important, since the impact of an outbreak will vary across geographic locations.

As in any crisis planning, security must be an integral partner with other company entities in planning for a possible H1N1 pandemic. Security must be involved in decisions for alternate work environments or locations for employees, work-from-home strategies, procedures for distancing at-work employees from the risk of infection, restriction or cancellation of non-essential business travel, and possible disruptions while traveling overseas. Security must have an understanding of human resources, legal and operational concerns prior to implementing their security procedures.

Communicate the Risks

Overseas travelers should be provided with information on what to expect if they are confronted with a suspected pandemic flu situation while traveling, and plans should be in place for the care of business travelers infected while they're away.

It is important to communicate to employees what to expect if the company and community are impacted by H1N1. For example, if schools are closed, what impact will this have on the workforce? If other businesses in the community are closed, will this impact the company's supplier or customer base, and will employees want to know why their company is not in sync with the community? With these external conditions influencing the business, the senior security executive should have networking in place with other corporate security executives and their counterparts in the public sector. Employees must have confidence in the information they are receiving, and this can only be accomplished with good coordination between company components and also with outside agencies.

Since security needs to maintain its staffing levels and its capability to protect company assets, consider the impact the pandemic may have on security personnel. Security personnel should be thoroughly briefed on company policies, personal protection, and how to respond to suspected flu cases, and they should be provided with appropriate protective gear. A good idea is to conduct a tabletop exercise on a pandemic scenario with key members of the team to discuss responding to a pandemic. This will help to improve the team's response and also to illuminate any deficiencies in the plan.

There are many resources freely available to assist security and the crisis management team in their preparations. The government Web site www.pandemicflu.gov contains extensive planning documents, including checklists for businesses as well as individual and family planning guides.

Guidance for businesses considering stockpiling antiviral drugs can be obtained at www.flu.gov/vaccine/antiviral_employers.html. Security can also obtain information from the Overseas Security Advisory Council (OSAC) http://www.osac.gov/ or the CDC travel website www.cdc.gov/travel on overseas travel situations. SECURITY

About the Columnist

Rad Jones is an academic specialist in the School of Criminal Justice, Michigan State University; retired U.S. Secret Service agent; former international security manager for Ford Motor Company; and Security Executive Council Emeritus Faculty. For more information about the Council, visit www.securityexecutivecouncil.com/?sourceCode=secmag