

Pandemic of Fear: Thinking about disaster recovery planning

By Craig Lucca

Many see the pandemic preparedness questionnaires as a sign that organizations recognize how they could be affected. Though I agree that on some level the proactive response merits some praise, I find the overall routine of pandemic questionnaires somewhat alarming.

As a security professional for a large financial services company, I frequently respond to client questionnaires regarding everything from security standards to regulatory compliance. Within the circle of professional contacts I maintain, the topic of an avian flu pandemic recently came up. Many of us have received pandemic preparedness questionnaires from clients, and many see the interest in this topic as a sign that organizations recognize how they could be affected. Though I agree that on some level the proactive response merits some praise, I find the overall routine of pandemic questionnaires somewhat alarming. As my opinion surely differs from the majority and is likely to elicit some controversy, please allow me to explain.

I am well aware that there is a growing concern about a possible pandemic caused by a variant of the H5N1 strain of avian flu. As both a security professional and a New York State emergency medical technician (EMT), I have been privy to multiple facets of how an outbreak would not only affect the global economy, but more importantly, cause serious loss of life. However, it is important that anyone concerned about avian flu spend time examining the medical history before subscribing to what many in the media have painted as the end of the world. There is a lot of research out there that makes it pretty clear that the likelihood of H5N1 mutating into a human-transmittable form is rather slim. Dig in to the Centers for Disease Control and Prevention (www.cdc.gov) and World Health Organization (www.who.int) Websites, or seek out the many reputable pa-

pers available through a well-executed Google search, and you'll find some pretty compelling and rather optimistic research.

As much as I don't want this article to be about the statistical possibility of H5N1 mutating into a species-jumping form, I think it is worth noting a few statistics easily available from the CDC and WHO Websites. In the United States approximately 36,000 people die each year from complications brought on by the seasonal flu. Approximately 1,000 to 3,000 people are infected each year with bu-

bonic plague; about seven to fifteen are infected in the United States each year, and one or two die as a result. Less than 200 people worldwide have died from avian flu since 2003. Granted, the potential for fatalities should H5N1 mutate are significant, but it's likely a vaccine will be available to treat such an outbreak.

At what staffing level can businesses continue to deliver services, and what alternative methods are in place, should that level be exceeded?

What concerns me about the recent wave of avian flu preparedness questionnaires is that they focus on the causes that would invoke Business Continuity Planning or Disaster Recovery (BCP/DR) plans and not the effects. In my opinion, a pandemic outbreak would be no different from any disaster, which could affect the resources every organization relies on. Let me elaborate on why I believe focusing efforts on addressing specific responses to the particular nature of such a pandemic is impractical and ineffective.

People, processes and technology make up the foundation of any good planning effort, be it tactical or strategic. BCP/DR plans should identify these resources, determine which ones are critical,

and plan for their continued availability during a declared event. It seems that in the years since 9/11 and the northeast US blackout of 2003, and given the recent increases in natural disasters, many organizations still don't understand that effective BCP/DR plans aim to address the effects of events rather than the causes.

Regardless of the specific cause of an event, whether chemical, biological or even nuclear, BCP/DR plans should make provision for short- and long-term continuance of operations. A pandemic may bring unique factors in how it causes an event to be declared, but ultimately the strain on staff and resources is similar to that of a biological event or even a regional natural disaster. BCP/DR plans that attempt to avoid the impact such an event will bring are doomed to fail.

One pandemic questionnaire I reviewed asked if Purell and Tamiflu would be offered to employees as a preventative approach. Since preservation of life is the absolute foundation of any business's BCP/DR plan, stocking up on Tamiflu as a means of maintaining staff levels does not make sense. Besides the potential legal exposure that may come about from distributing such items, there are other factors that can't be solved with preventative measures. Not least of these are employees who would refuse to enter potentially contaminated areas – and who could blame them; employees who would be tending to sick or infected family members; and the possibility of local, state and even national quarantine restrictions. Additionally, there has been significant debate as to whether or not Tamiflu would even be effective.

Having affiliations and advanced training in emergency medical services, I fully appreciate how delicate people are. The experiences I've had responding to anthrax scares, SARS and tuberculosis, as well as participating in weapons of mass destruction drills, are all factors I consider when developing BCP/DR plans. I believe it's important that we educate our workforce on the topic of avian flu, but we must do so in a way that doesn't add to their fears. There are unfortunately numerous threats out there, which, given the correct set of circumstances, could seriously harm our society. However, evolution has provided us with many defense mechanisms to combat diseases and viruses, and advances in medical science continue to make up for those we cannot combat. Additionally, researchers have been investigating H5N1 for a few years now; it's the media that has only recently begun to popularize it.

As professionals, we must not forget the lessons learned from the recent events in the Gulf Coast area of the US. As multiple hurricanes pounded Louisiana, Mississippi and Texas and caused billions of dollars in damage to infrastructure, resources nationally were pushed beyond their breaking points. Emergency response agencies were unable to assist, and many people and businesses were left to fend for themselves. How would a pandemic be any different? Wouldn't organizations see sharp increases in employee absenteeism? Couldn't organizations be inhibited or even barred from allowing employees to enter or leave their facilities due to emergency operations or public safety concerns?

The question organizations should be asking of themselves and their critical vendors and suppliers is, what provisions do they have in place to address high rates of absenteeism among staff? What steps has your organization undertaken to identify alternative processing locations should your primary facility become inaccessible or inoperable? How long can you sustain operations under the most extreme adverse conditions? As security professionals who understand concepts such as the availability principle, it is essential that we assist our organizations in focusing efforts on dealing with effects, and not necessarily the causes which activate BCP/DR plans. Ask the question, what level of absenteeism can we sustain and still deliver products and services?

Performing a proper business impact analysis (BIA) is essential in identifying the critical resources necessary to maintain operations. By fully understanding the resources and processes necessary to maintain operations should an event occur, accurate BCP/DR plans can be developed to sustain operations, meet the needs of the business, and protect its workforce. Businesses do not need a specific plan for a hurricane vs. a pandemic when the outcome of these events would lead to similar problems for facilities and personnel. A proper BCP/DR plan should identify alternative processing facilities and methods for providing staffing to maintain operations. Additionally, plans should already provide alternative means for workers to carry out job responsibilities, whether it's through telecommuting or cross-trained employees who would suspend their less essential functions in order to assume those deemed critical at the time. Whether the event is a fire, flood or pandemic, a solid remote access infrastructure can address those factors which could inhibit a workforce from accessing their facilities.

Availability is a critical factor within an organization's security program. Maintaining system availability requires significant resources and accurate planning to achieve the recovery-time objectives identified in an organization's BCP/DR process. Focusing on ways to prevent or avoid events, as part of a BCP/DR strategy, is ineffective. There are too many scenarios to factor for, all resulting in similar outcomes. The circumstances responsible for causing disruption of services will vary greatly and become considerably more difficult to manage as our society and world continue to evolve and change.

Organizations that spend time trying to figure out how to beat a pandemic are missing a more critical issue: At what staffing level can businesses continue to deliver services, and what alternative methods are in place, should that level be exceeded? If the possibility of a pandemic has been the first issue to make you question your BCP/DR plan's effectiveness, then something is missing from your BIA process. Budgets and security personnel are already stretched pretty thin. Spending time questioning whether your organization, or that of a critical vendor or supplier, is capable of maintaining operations should a specific set of circumstances unfold, is not an efficient or even practical approach. Establishing what thresholds would need to be exceeded before your organization or that of a critical vendor or supplier could no longer deliver service, will provide a better benchmark for assessing risk.

Lastly, it's important that we as security professionals remember another important point: credibility. As security professionals we are obligated to maintain an objective view of emerging threats and to react accordingly. By joining the bandwagon of avian flu pandemic hysteria, we are increasing panic, using our resources in a less than efficient manner, and doing a discredit to our profession.

About the Author

Craig Lucca, CISSP, CISA oversees information security and is responsible for the global identification, design and implementation of – and compliance with – corporate information security programs for a large financial services firm. In addition, he acts in an advisory capacity to the firm's lines of business regarding information security best practices and the interpretation of security requirements of new and ongoing development efforts. He can be reached at craiglucca@snet.net.