Information Systems in the Time of Flu

I wrote the article below 14 years ago as the H5N1 virus, familiarly known as avian flu, was threatening the world. As I said then, I only have useful advice to offer in business continuity management and information technology so that was what I did then…and now again. Sadly, but predictably, we are facing a similar threat again today. It was predictable because in this century, only 20 years old, we have had SARS (2002), MERS (2012)—both of which are coronaviruses—avian influenza (2006) and swine influenza (2009). It was only a matter of time before a novel virus broke out internationally, and now it has.

Implicit in much of what I wrote then was that there was still time to prepare. In some localities, such as New York (where I am sitting as I write this), Milan, Teheran and Wuhan, we can only react. Our opportunities for preemptive action are in the past. Still, everyone everywhere should get underway immediately, giving as many workers as possible the ability to work remotely; reinforcing our telecommunications networks; training people to keep systems running; and generally considering how IT will function amidst widespread absenteeism. If we do not take advantage of the little advance time we do have, for goodness' sake, when will we ever?

What follows was originally published in the *Information Systems Control Journal* (the former name of the *ISACA® Journal*), vol. 4, 2006.

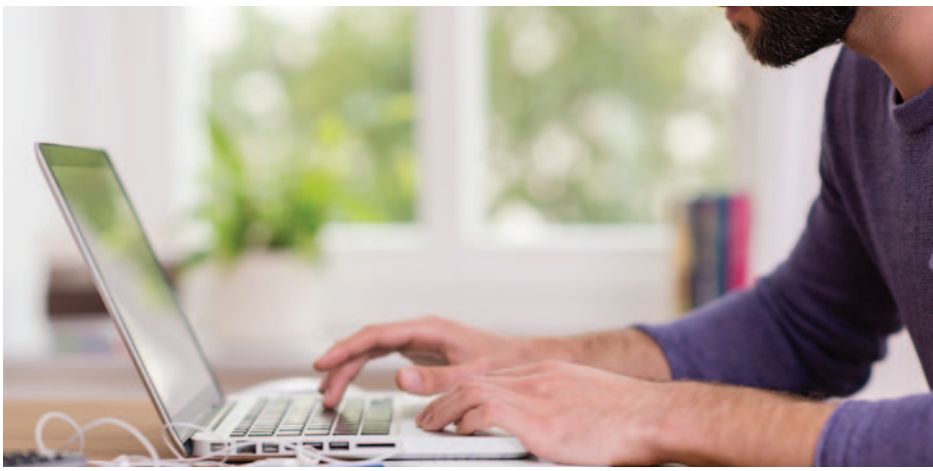
I sincerely hope that by the time this is published, an outbreak of a pandemic affecting human beings is still in the future. Sadly, I do not think it is speculative. Every researcher, virologist, epidemiologist and public health specialist I have spoken with is certain that something will occur, whether it be avian flu currently affecting birds worldwide or some as-yet-unknown disease. Having no medical background myself, I will avoid any statements about the disease itself. If you want advice on what to do about your health, consult your doctor.

I am not in the public health field either, so if you are concerned about the ability of doctors and hospitals to withstand the surge of demand that a pandemic will bring, speak with your local medical authorities. And I am certainly not a politician; the ability of our society to manage the inevitable disruption that would be caused by a widespread outbreak of a communicable disease is the province of your government officials.

I do know something about planning to run a business during an emergency, though. And since this is the *Information Systems Control Journal*, I will focus my comments in the rest of this article on the positive and negative effects a pandemic might have on information systems.

Remote Access and Social Distance

Remote access, combined with the Internet and virtual private networks (VPNs), is viewed by many as the best way to achieve the goal of social distance.[1] If people are able to work from home, they can continue to be effective if they are well



Steven J. Ross, CISA, AFBCI, CISSP, MBCP
Is executive principal of Risk Masters International LLC. Ross has been writing one of the *Journal's* most popular columns since 1998. He can be reached at stross@riskmastersintl.com.

Enjoying this article?

- Read *Enforcing Data Privacy in the Digital World*. *www.isaca.org/enforcing-data-privacy*
- Read the latest ISACA Now blog post. *www.isaca.org/blog*
- Learn more about, discuss and collaborate on navigating COVID-19 in ISACA's website. *https://www.isaca.org/go/covid19*

enough to do some work or if they need to stay with family members but are not ill themselves. Many companies enable teleworking (the latest jargon) today, but in the majority of cases, it is for some people to use some of the time. It is far from clear whether many companies have the capacity—not the capability—to enable teleworking for most of their personnel most of the time.

What would be needed, therefore, is a significant expansion in the number of ports, telecommunications bandwidth, dissemination of VPN software and certificates, and the application and infrastructure software to enable people to be effective from home. All this must be implemented in advance, and it has a cost that must be justified. I have observed that the *insurance model* does not work in convincing senior executives to spend a lot of money. After all the scares in recent years—including Y2K, terrorism and global warming[2]—it is difficult to make chief executive officers (CEOs) believe that the world is coming to an end.

However, the *investment model* does work. It is necessary to demonstrate the current benefit of expenditure, the return on investment (ROI), to get the money needed. Fortunately, there is a strong argument for expanding remote access: it creates a more mobile workforce. Those who can work wherever they are, whenever they want, tend to be more productive.

There is a security issue associated with access to the company's intranet over the Internet. If the computers that contain the VPN software are company-issued, with standard firewalls and virus protection, remote access is functionally equivalent to access from within the office. However, if it is expected that personnel will work from home on their own computers, the situation is rather different. Assuming that no one wants to lower security, there must be a mechanism for checking that employees' home computers have the appropriate security software. Moreover, there must be sufficient compatibility between the operating systems and other software (e.g., word processing and spreadsheet, applications) to let people work.[3] If these conditions cannot be met, management needs to consider either issuing loaded laptops in advance of a pandemic outbreak or permitting personnel to obtain compatible computers at that time. This, in turn, raises questions concerning the distribution of software. Taken together, these are not insuperable problems, but they are far more difficult to resolve in a crisis than beforehand.

The Extended Enterprise

Of course, working at home is not a panacea. In the words of Professor Michael Osterholm of the University of Minnesota (USA), one of the foremost researchers in the field, "You can't make steel from home."[4] Moreover, just as companies do not currently anticipate all their personnel remotely accessing their systems all the time, there are significant questions as to whether the Internet can tolerate such expanded, global, simultaneous use. How many concurrent sessions can any particular Internet service provider (ISP) accept? My personal opinion is that access will become more difficult but not impossible; the Internet will slow but n ot stop.

That is, it will not stop for everyone. But the Internet travels over facilities operated by telephone companies and cable operators. They, like every other business, will be facing large temporary labor shortages. For the most part, data, voice and video networks run unattended, but circuit packs fail and lines are cut, far more often than you might expect. Today, someone replaces the pack or repairs the line, often without customers being aware of the interruption in transmission capability. But if a third or more of telecommunications vendors' personnel are unavailable, these fixes will take longer to initiate and complete. Some people may be left looking at blank screens.

Keeping Systems Running

And just as workers at a central office will become ill, so will operators and technicians in companies' data centers.

Simply put, how many people are needed to run the systems on the third shift, and what can a company do if those people cannot or will not come to work? There is little that can be done if businesses wait until a pandemic arrives. But if they start planning now, they can begin to cross-train personnel to operate and manage data centers when there is widespread absenteeism. Application programmers may be valuable in keeping their systems running, if they are trained to do what operators do. Even IS auditors might be pressed into service!

> "THERE IS LITTLE THAT CAN BE DONE IF BUSINESSES WAIT UNTIL A PANDEMIC ARRIVES."

The moral is not the need for more operators and technicians, but rather that waiting until a pandemic strikes will not suffice. If you accept the prediction that one-third of the population may be affected—more likely to be sick than to die, to be sure—that means one-third of everyone (operators, auditors, managers and senior executives) will be unable to work under normal circumstances. Thus, decisions that should be made by senior levels of management will have to be made by subordinates. It is unlikely that a coherent response to such a crisis will emerge under these circumstances.

Fortunately, preparing for a pandemic is an extension of planning for any other contingency that might affect the ability of personnel to access their normal workplaces. The plans that are needed to continue operations when disease is present are not very different than those for a strike, catastrophic weather or even your home team winning the championship. True, there is a medical component to it, and it will last longer than a victory parade. For those of us who have dealt with disasters, viruses, and subway strikes, the possibility of a pandemic presents management problems; we have beaten them in the past, and we will this time as well. *But only if we begin now,* before a pandemic arrives.

Endnotes

1 I am not sure who originated the term, but it is widely used in epidemiological circles. A good reference, worth quoting a bit here, is the World Health Organization's *WHO Pandemic Influenza Draft Protocol for Rapid Response and Containment*, *www.who.int*, which says: "Modelling studies have indicated that certain 'social distancing' measures might increase the likelihood of successful containment. Such measures aim to increase the social distance among people in an outbreak zone and thus reduce opportunities for transmission to occur. Like quarantine, these measures are socially disruptive, and some may cause considerable distress or discomfort in the affected population. Moreover, their actual impact on transmission patterns has not been fully documented in scientific studies."

2 Of course, these are, or at least were, real threats. Many have forgotten the millions, probably billions, of staff hours that went into making 1 January 2000 seem like just another day. The difference is that in 1999, we did not know what would happen, but we knew exactly when. With a pandemic, we know what will happen—many people will fall ill—but we do not know when.

3 Ross, Steven; "Virtual Private Infrastructure," *Information Systems Control Journal*, vol. 6, 2001

4 Summit on Business Planning for Pandemic Influenza, Minneapolis, Minnesota, USA, 15 February 2006. In the interests of full disclosure, Professor Osterholm is a consultant to Deloitte & Touche.