National Security Cyberspace Institute

CyberPro

July 2009

Keeping Cyberspace Professionals Informed

THE PRUDENT CIO AND THE PANDEMIC

BY DR. JAMES KASPRZAK, NATIONAL DEFENSE UNIVERSITY
& DR. MARY ANNE NIXON, WESTERN CAROLINA UNIVERSITY

What steps should a prudent IT manager take to meet the present threat of a swine flu pandemic?

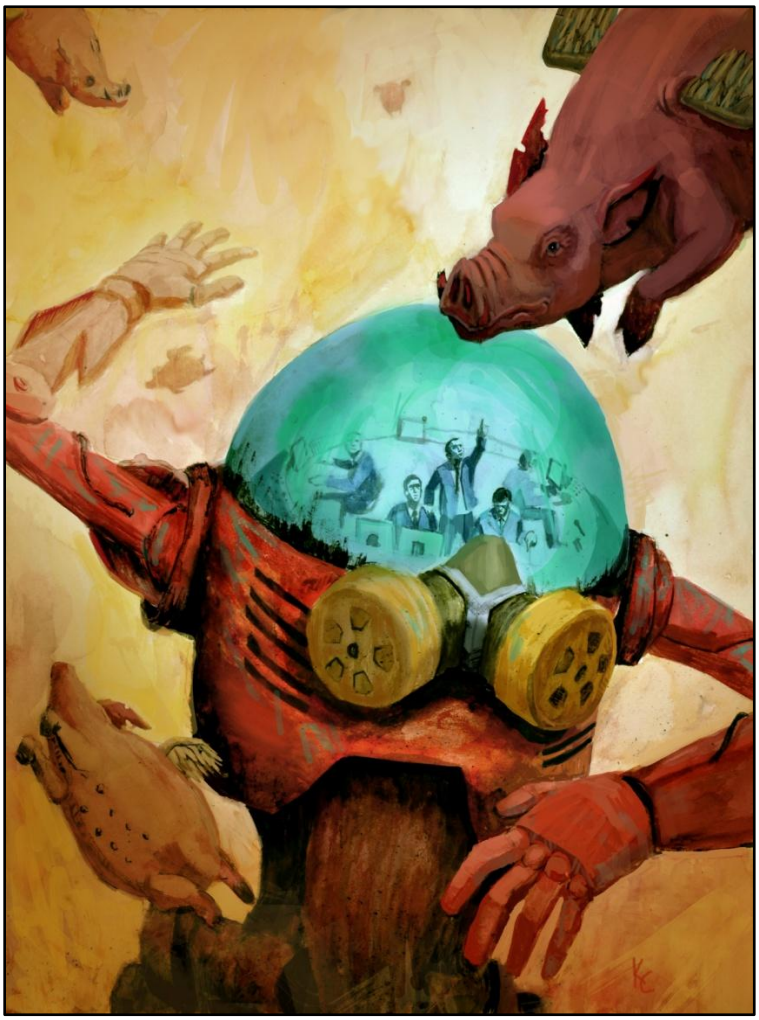

Illustration by Kenny Callicutt, www.callicuttart.com.

It is difficult to assess the risks of a pandemic by traditional risk assessment methodologies, if only because newly-emerging viruses have "strategies" of their own, and can change unpredictably to adapt to new environments and meet new conditions. Because pandemic risks are so uncertain, a manager may hesitate to waste time and money preparing for such threats, especially when other needs are so certain and so pressing. And then there is the risk to the manager's reputation: only so many times can he or she call, "Wolf!" and maintain credibility for the time when a real wolf shows up. Finally, there is the unusual nature of the pandemic threat and the measures to be taken against it. We can't defend against disease by the usual continuity of operations measures: crowding people into bunkers, backing up files or designating alternate sites.

Managers currently have a window of opportunity in which to prepare for the effects of the latest viral threat – the H1N1 "Swine Flu" virus. Influenza viruses generally disappear in warm weather and re-emerge in the late fall through winter months. When they return, they have often mutated and sometimes reappear in a more virulent and dangerous form.

The famous "Spanish Flu" virus of 1918 first showed up as a relatively mild illness. It faded away and returned months later in a second wave, killing more than 50 million people worldwide. The current strain of Swine Flu worries health authorities because it is pieced together from portions of several

other viruses found in pigs, birds and humans, and is highly unpredictable. Even more disturbing, it shows one of the distinctive characteristics of its deadly cousin, the Spanish Flu: it affects those with very healthy immune systems worse than children or elderly victims. The Centers for Disease Control (CDC) reports that the average age of H1N1 patients is 12 years old, but those patients who are affected so severely as to require hospitalization are on average 20 years of age.

Are there any low-key, low-cost preparations which a CIO or IT manager can take to prepare for such an uncertain, but potentially catastrophic, threat? To begin with, pandemics have precursors that warn of the oncoming danger. A virus doesn't travel the world infecting millions in a single day; it is likely to infect small numbers of people weeks or months ahead of the large mass of the population. An observant manager will therefore have time to implement an existing pandemic response plan.

Swine Flu has spread rapidly, but the infection itself has a relatively low mortality rate, comparable to our annual influenza epidemics. If the mortality rate from this unpredictable virus increases in the fall and early winter, this would be a serious indicator of danger to come.

Pandemics affect people inside and outside the organization. Key individuals – from the head of the organization, down through the manager of network operations, to the guard at the front desk – may be unpredictably absent for long or intermittent periods. When a family is hit by an infectious disease, one member after another may be affected in a series of illnesses. If the sickness requires quarantine or home confinement, an employee might be absent for weeks.

In addition, local governments have considerable power over employee availability, and the effects of the pandemic will not be geographically uniform at any one time. While one nation may ground all airline traffic within its territory, another may have no limitations on commerce. While a major city may be open for business, all schools in the suburbs could be closed. In some jurisdictions, nursery and elder care may be unavailable, or mass transportation systems may be shut down. Local health officials generally have the authority to forbid gatherings in churches, theaters and businesses. Even stores and restaurants could be closed.

The CIO and his or her IT personnel have some special responsibilities during a pandemic. Health authorities call for social distancing as one of the key public responses to a serious pandemic. Social distancing calls for fighting contagion by limiting physical contacts between persons to the minimum essential interactions. For example, gatherings such as meetings and conferences would be avoided. Most scenarios for social distancing are heavily dependent upon IT technology in all of its forms: computers, telephones, teleconferencing and Internet communications. During a pandemic, an organization's IT personnel and infrastructure may be its most critical assets.

By all accounts, threats of a serious Swine Flu pandemic are four to six months out. What should a prudent CIO be doing now?

Dust off the Plans

The pandemic plan provides for an orderly continuation of organizational functions in emergency conditions of contagion. Who declares that an emergency exists for the organization and when it is over? For pandemics, these determinations may not be easy or simple. Which countermeasures should

be taken at different stages? Are any operations to be suspended? The emergency data in the plan – contact information, names and suppliers – should be updated now, and kept up to date over the next few months. How will the organization put out news to all members of the organization? Will there be a special website, use of a telephone notification system or mass e-mailings?

At this stage, someone in the organization must be designated to monitor pandemic information and preparations. This includes checking the websites for the World Health Organization and the Centers for Disease Control. Find out if local health and civic authorities have websites or other standard channels to distribute information in an emergency. Get key phone numbers. Until there are further developments, monitoring efforts will require only a few hours each week for one person.

Policies

Emergency policies should be developed now for quick implementation as required. The organization should consider how best to support employees and their families. Will the organization continue to pay an employee who has no sick leave? If not, employees will be tempted to conceal their illnesses and come in to work because they need the money. Sick employees should be discouraged from coming to the central worksite – by health screening at the door, if necessary. At some point, management may prohibit non-essential meetings, discontinue group training and discourage travel by airlines. The Internet contains dozens of websites listing policies to be considered and emplaced for pandemic emergencies, including policies on absenteeism, overtime and hazardous duty pay. The CDC, for example, has posted a "Business Pandemic Influenza Planning Checklist" at www.pandemicflu.gov/plan/businesschecklist.html .

Succession

Key individuals and their potential successors must be named. In the Information Technology Department, successors should be two, three or more people deep. Succession plans should not only include the IT manager, but all individuals whose absence would seriously disrupt the business operations of the greater organization. This includes the man with the keys, the lady with essential security clearances or the only one authorized and enabled to make payments to suppliers.

But a succession plan is not simply a piece of paper. Each designated successor needs to have sufficient training and access to the resources required to do the job: the keys, the combination to the safe and possession of a company credit card. To maintain a sufficient level of IT skills during a pandemic, many people may have to be cross-trained. Now is the time for that training.

Maintenance and Supply

Just as no human being should be a single point of failure for the IT department, there should be extra consideration given to the supply, repair and replacement of IT equipment. During a pandemic, there may be delays in supply, distribution or delivery. A relatively small float of spare equipment, especially of key components, will go far to ensure the continued operation of your systems.

If the organization plans to let its employees telework during a pandemic, it may need a different mix of equipment and supplies from normal operations. Individuals should check the usability of their personal telework equipment. Whenever possible, buy IT equipment and supplies you were going to get anyway – just stock the items a few months in advance.

In addition, you might want some support items needed in a pandemic: trashbags, cleaning equipment, rubber gloves and sanitary wipes. These items are inexpensive, and most can be used for other purposes if not needed for an emergency. Note that when the World Health Organization announced the emergence of Swine Flu, some health items, like face masks and sanitary wipes, disappeared from the shelves of the large retailers for almost a week. It may also be useful to make extra keys, credit cards and access badges for an emergency and store these in a secure place.

There are some sites, such as central computer rooms, network operations centers and data storage facilities which must remain operational even if only at a low "manning" level. Workers might come to the worksite scattered over shifts in a 24-hour period, or do support work from decentralized locations. Commonly-used equipment or surfaces would be decontaminated with wipes and cleaning materials.

How do such workers, and their teleworking customers obtain needed supplies and maintain their equipment and services over an extended period of time? Logistics support must include pre-determined quantities of spare computers, cell phones, Internet access cards, external access to intranet files, etc., to support remote workers. Transportation may be a separate problem.

The Supply Chain

That brings us into consideration of all the people outside the organization who support it with their supplies and services. Long before a pandemic, the CIO needs to determine the robustness and dependability of current suppliers and service providers, including Internet service providers, wireless and other telecommunications services.

Should there be some guaranteed service level agreement? What assurance do we have that our organization will have priority service when every customer will have urgent requirements? Should we contract with secondary suppliers?

Remember also that employees working from home also have ISPs and service providers. Should you worry about these? In a pandemic, there may be many, many employees simultaneously working from home – a workload that our telecommunications systems were not designed to support.

Communicate

Finally, this is the time to brief all employees on how the organization plans to meet the pandemic challenge, and how it will support its employees and their families. At this stage, we are concerned only with the succession plans of the organization and the general concept of operation during a pandemic. There will be time later, if required, to train on medical precautions and details of policies. Now we are concerned with mobilizing the organization's human resources and obtaining their confidence and support for the tasks that may lie ahead.

About the Authors

Dr. James E. Kasprzak is a professor in the Information Operations and Assurance Department at National Defense University, Washington, D.C.. Prior to teaching at NDU, he spent 20 years in a series of information resource management policy and planning assignments in the U.S. Army. He was awarded the U.S. Army's Civilian Meritorious Service Medal for "Saving the Army $100 million by automating its

administrative information systems." Dr. Kasprzak specializes in applications of telecommunications, computers, privacy and access, and eGovernment. Recent publications include "Women and the Web: An Update," "Providing Feedback to Students in Distance Education" and "The Identity Theft Nightmare." He has presented widely on issues related to identity theft, privacy and continuity of operations.

Dr. Mary Anne Nixon is a professor in the Global Management and Strategy Department at Western Carolina University, in Cullowhee, N.C. She is an attorney and member of the North Carolina Bar. She completed the U.S. Department of Defense Systems Advanced Program Management Course, the highest level of education for military and defense industry program managers, and was designated a Certified Professional Contracts Manager by the National Contract Management Association. Dr. Nixon has served as an educator and consultant for Fortune 500 corporations in telecommunications, energy and computer industries. She is a member of PMI and has PMP certification.