INFORMATION SECURITY®

ESSENTIAL GUIDE TO

Pandemic Planning for H1N1

Here's how to prepare for a possible swine flu outbreak so your business can continue to operate smoothly and securely.

INSIDE

TechTarget
The Technology Media
ROI Experts

INFOSECURITYMAG.COM

ESSENTIAL GUIDE

contents

PANDEMIC PLANNING

FEATURES

PANDEMIC PREPARATION— A User's Perspective

Here's six steps you can take now in order to be ready for H1N1.

BY ERNIE HAYDEN

PANDEMIC PREPARATION. We've heard about this issue in the disaster planning ranks for the past few years, first starting with the avian flu concerns and now with the swine flu otherwise known as H1N1. Albeit it is easy for most managers and executives to get jaded over these topics—especially when the "fear, uncertainty, and doubt" mongers are actively stirring up concerns. Skepticism aside, there are some things that any and every company should do as part of their pandemic preparations.

PROTECTING THE CIAA

As a security professional focus is always on assuring the C—Confidentiality, I—Integrity, and A—Availability of the data. During the pandemic preparations there is no change to this focus; however there are some added dimensions of concern for the infosec professional—especially in the availability arena.

Step 1: The Pandemic Committee

A company should implement a pandemic preparedness committee made up of Human Resources, Executive Management, a Union Representative, Physical Security, Facilities, Information Technology and Information Security.

Step 2: Liaison with Local Public Health Officials

The Committee should immediately reach out to the local public health organizations in order to take advantage of the calmer communications now so that the faster, more energetic conversations that will ensue are easier because the lines are established. In a similar manner, the facilities, IT and infosec staff should reach out to their peers and other regional organizations such as Information System Security Association (ISSA) or InfraGard to be certain that lessons learned and even key resources as part of preparation are shared.

Step 3: Prepare the Management

The Committee should begin to prepare the management for such issues as handling employee absence from the office (even if they are healthy but their family members are not), the ability to remotely work from home and rules for overtime and timesheet submittals under these circumstances, among other issues. Also, management needs to be encouraged to think ahead about contingency plans should key players be out of the office temporarily or permanently due to the flu.

H1N1 Statistics

The H1N1 influenza virus, first detected in April, was declared a pandemic by the World Health Organization (WHO) in June. According to the Centers for Disease Control and Prevention in the U.S., 27 states were reporting widespread influenza activity and almost all the influenza viruses identified so far are H1N1.

A report [http://www.whitehouse.gov/assets/documents/PCAST_H1N1_Report.pdf] released by the President's Council of Advisors on Science and Technology (PCAST) in August concluded that the H1N1 flu is unlikely to resemble the deadly "Spanish flu" pandemic of 1918-1919. Still, the current virus strain is serious health threat, unlike the swine flu episode of 1976, the group said.

According to the PCAST report, the impact of a fall resurgence of H1N1 is impossible to predict, but an epidemic could infect 30% to 50% of the U.S. population, lead to up to 1.8 million hospital admissions, and cause between 30,000 and 90,000 deaths, mostly children and young adults. Seasonal flu usually kills 30,000 to 40,000 people in the U.S. annually, but mostly among people over 65, the report noted.

—MARCIA SAVAGE

Step 4: Prepare the Employees

Employees need to be briefed by HR, their managers and other individuals such as union representatives on the processes for reporting absences. Also, the employees need to understand how to use such communication tools as Outlook Web Access (or Webmail) and phone bridges in order to sustain communications for the business. These last two items can be trying on the IT and infosec staff need to assure that accounts are pre-established, laptops and other equipment are issued as necessary, and protocols to avoid overtaxing the IT and communications infrastructure are observed.

Step 5: Run an Exercise

Although it doesn't seem practical, it is possible to run an exercise to help management understand the implications of a true pandemic on their business. In one case, the Port of Seattle ran a pandemic exercise for the senior management team. This exercise was run by the Pandemic Committee and the CISO. To better help the management understand how hard a pandemic can hit the organization, the Seattle team took a list of the Port employees and arbitrarily marked every third person as being absent. Then, the list was re-sorted by department and each department manager was given their list of those "missing in action" at the beginning of the exercise. As part of the exercise each manager had to explain the implications of those missing due to the flu and how they would need to handle their day-to-day tasks while key personnel were missing. As a result of the exercise, managers understood in a dramatic, visceral manner that they needed to be better prepared should the payroll person be out ill or the key shipping and receiving employee be absent, or the master customer service employee could not return to work.

Step 6: Implement the Preparations

The final preparations really focus on people, process and technologies. First, educate all staff. Secondly, implement a system to handle and assess daily absence information. In other words, determine who is out ill; assess if there are any patterns that show an entire department could be sick or a geographic area could be hit hard.

For technologies, the IT and infosec staffs need to be sure that the VPN and email systems are up and running and tuned to allow for major remote access loading. Also, the office phone system needs to be prepared for optimal phone forwarding such as to the new department lead or to cell phones and other desk phones. Facilities staffs need to be assured that such services as mail, trash removal are handled with normal vendors or contingency service providers. Lastly, there needs to be a process to ensure that the status of the workplace is communicated to customers as well as employees in order to be sure the "all clear" is communicated and that emergency requirements from customers can be fulfilled.

For technologies, the IT and infosec staffs need to be sure that the VPN and email systems are up and running and tuned to allow for major remote access loading.

Your best approach is to stay on top of the issues, get a coordinated approach within the company, and don't focus exclusively on human resources when so many other players such as IT, facilities and infosec are needed to help assure that the data is protected and businesses run smoothly. ▸

Ernie Hayden is the founder and owner of 443 Consulting, LLC, an enterprise focused on providing quality thought leadership in the areas of information security, cybercrime/cyberwarfare, business continuity/disaster recovery planning, and research. Previously Hayden was Information Security Strategic Advisor in the Compliance Office at Seattle City Light. Prior to his arrival at Seattle City Light, Hayden was the Information Security Officer (ISO) for Group Health Cooperative—one of the largest private employers in Washington State and one of the largest healthcare systems in the area and the Chief Information Security Officer for the Port of Seattle.

SWINE FLU PUTS SPOTLIGHT ON PANDEMIC PLANNING

The possible outbreak has many firms on alert and preparing to activate their pandemic response plans.

BY MARCIA SAVAGE

AT CIGNA CORP. an emergency response team of medical and business leaders meet daily to assess the situation and determine what steps need to be taken, said Gloria Barone, a spokeswoman at the Philadelphia-based health insurance company.

CIGNA has developed an action plan to prepare for the consequences of a swine flu pandemic, which includes an existing emergency system that the company said is easily activated to help facilitate care for its members in the event of a pandemic. The company's business continuity plan includes the ability to allow many employees to work from home during a pandemic. Also, CIGNA said it will implement travel guidelines or restrictions as needed to minimize spread of the flu.

The company said it had an internal clinical committee in place for some time to develop policies and procedures in the event of a flu pandemic.

John Carlson, senior vice president of regulatory affairs for BITS, a nonprofit financial-services industry consortium and division of The Financial Services Roundtable, said financial institutions are monitoring the swine flu situation and activating elements of their business continuity plans. The Financial Services Sector Coordinating Council is actively working on the issue with federal officials and regulators, he said.

A security manager at a West Coast-based bank said his company is monitoring the outbreak on multiple official state and federal websites.

"We already had a plan based on the avian flu," he said. "We're pretty much prepared."

Most companies that have taken the avian flu pandemic threat seriously should be prepared, he said. Experts have warned in recent years about the pandemic potential of a strain of avian influenza, the H5N1 virus.

Unlike other businesses that can send employees home to work remotely in the event of a pandemic, the bank needs to stay open and deal with the public, said the security manager, who requested anonymity.

Consequently, the bank's pandemic plan involves being able to stay open and reducing the number of employees who are potentially exposed by allowing them to work remotely. With the swine flu outbreak, the bank has been making sure branch hand sanitizers are full. Any disaster plan relies on employees following instructions, he noted, and most bank employees understand they should wait for direction from their supervisor.

The information security officer at an East Coast-based bank said his company updated its pandemic plan last year and currently following guidelines from the WHO and its internal HR process.

"The most important thing is to not only have a plan, but to test the plan," he said. "No company wants to disrupt their operations for planning but it's crucial."

John Copenhaver, president and CEO of DRI International, a Conway, Ark.-based provider of education and certification for business continuity professionals, said the organization is fielding questions about executing pandemic plans, indicating that many companies are in a heightened state of alert if not already activating initial stages of their pandemic response plans.

Influenza Pandemic Resources

FFIEC Interagency Statement on pandemic planning
http://www.ffiec.gov/press/pandemicguidance.pdf

Federal government website with pandemic information, managed by the U.S. Department of Health and Human Services (HHS). Includes influenza planning guidance
http://www.pandemicflu.gov/index.html

World Health Organization
http://www.who.int/en

Centers for Disease Control and Prevention
http://www.cdc.gov

BITS
http://www.bits.org/downloads/Publications%20Page/PandemicResources.pdf

–COMPILED BY MARCIA SAVAGE

"Most of the larger financial institutions have some kind of pandemic/influenza plan or at least a pandemic overlay to their existing business continuity plans," he said. "But I don't know if I would say they're all prepared to the extent that they need to be prepared."

Pandemic planning involves dealing with the business impact of potential absenteeism—employees who are sick and can't work or who are afraid to come to work for fear of getting sick, Copenhaver said. Other elements include securing certain facilities from people who are obviously sick, how to help infected employees and their families, and how to help employees who are traveling abroad, he said.

Even if the flu doesn't develop into a worst-case scenario, companies are already dealing with effects from the outbreak in terms of some school closures and travel impacts, Copenhaver said.

"The jury's still out on how bad this is going to get," he said. "We don't know what the mortality rate will be. If this is something like ordinary influenza in terms of its mortality rate, it will still have an impact on us, but if it turns out to be something more severe, like the Spanish flu outbreak in 1918, we'll see just how well prepared we are."

Seasonal flu kills approximately 36,000 people in the U.S every year, according to the CDC.

BITS' Carlson said the financial services industry has taken a number of steps to prepare for a pandemic. Two years ago, the industry in conjunction with the Treasury Department and federal regulators conducted a major pandemic exercise and documented their findings on pandemic-related absenteeism, telecommuting, communications and other issues, he said.▸

Marcia Savage is Features Editor for Information Security *and Site Editor for* *SearchFinancialSecurity.com*.

5 Mistakes Organizations Make in Their Pandemic Planning

Experts cite five areas where financial institutions could improve their planning for a potential H1N1 outbreak.

BY MARCIA SAVAGE

WITH THE H1N1 VIRUS THREATENING to hit hard this flu season, pandemic planning has become a priority for many organizations. A recent survey by the Pandemic Prevention Council of about 1,500 U.S. organizations showed that a slight majority report that senior management has stressed the importance of preparing for a possible H1N1, or swine flu, outbreak.

However, while 75% of those surveyed have business continuity plans, only 55.6% of private companies have plans that address the H1N1 threat.

The banking industry has done a better job than other industries in developing pandemic plans, said Richard De Lotto, principal analyst in Gartner Inc.'s banking and investment industries advisory services. "It doesn't take much research into the 1918 pandemic to realize that you need to take this seriously," he said, referring to the "Spanish flu" pandemic that killed more than 500,000 in the U.S.

The avian flu threat and a 2006 advisory on pandemic planning issued by federal regulators helped to spur pandemic planning in the financial industry. The FFIEC updated the advisory in 2007 with expanded [http://www.ffiec.gov/press/pandemicguidance.pdf] pandemic planning guidance. In April, the emergence of swine flu prompted an uptick in flu preparations. But experts cite several areas where financial institutions could improve their planning for a potentially massive H1N1 outbreak. Here are five mistakes banks make, or areas they overlook, in their pandemic plans:

1. NOT DOING ENOUGH

Even though financial services, as a heavily regulated industry, may be further ahead in preparing for a pandemic than others, many banks still don't have a comprehensive plan.

"The biggest issue is that the banks haven't really thought through it," said Ruth Razook, CEO of RLR Management Consulting Inc., a La Quinta, Calif.-based firm that provides IT, strategy and other services to community and independent banks. "They haven't taken that time."

Federal banking regulators are very serious about pandemic planning, she said: "The regulators are saying it will occur, that it's not a matter of if, but when. And if banks aren't prepared, it could get pretty ugly."

Specifically, regulators told her some financial institutions don't understand the difference between planning for business continuity and a pandemic. In the first, the building is gone but the people remain while in the second, the building is there but the people are gone. "They're not grasping the fact that you could be down 50% of your people," Razook said.

David Schneier, a compliance consultant who works with financial institutions, said he's yet to review "a truly viable pandemic plan." Most of the plans he's seen discuss possible pandemic scenarios but don't provide actionable steps in the event of a quarantine.

"What happens when a bank or credit union cannot staff their braches due to a severe outbreak? How will operations be maintained if offices are closed down and staff forced to work remotely? I suspect that much of what occurs will be ad hoc," he said.

Meanwhile, some large financial institutions that perform extensive pandemic planning at their corporate headquarters fail to extend the effort to their regional or local offices, said Brian Zawada, co-founder and director of consulting services for Avalution Consulting LLC, Cleveland, Ohio. They mistakenly believe they should focus their efforts on the locations with the most staff.

"You have to be consistent and able to show that preparedness activities are applied across the entity, no matter where or how many people," Zawada said.

2. LACK OF DEFINED POLICIES

Some companies don't have clear contagious illness policies, Zawada said. These policies clarify that if employees are sick, they stay at home and if they show up to work sick, their manager has the right to tell them to go home.

"Those that don't have such policies have managers running around saying, 'I have this person coughing up a storm. What do I do?' By the time they get an answer, it's too late and others are sick," he said.

Other policy issues that need to be decided on before a flu epidemic hits is how a financial institution plans to handle sick leave.

"One bank said they had an employee come back from Mexico and came to work with a fever. They sent him home. If he doesn't have any sick time left, does he get paid or not?" Razook said. "Banks should be figuring out what those policies are, and I don't think they are."

David Sarabacha, principal at Deloitte & Touche LLP and leader of the firm's business continuity management team, said companies vary widely in how they plan to handle sick leave.

"It stretches from, 'It's not our problem. We give a certain amount of time for sick or vacation days. If something arises, we won't give anymore'," to other organizations saying they'll give seven to 14 more days of time off, especially if they tell you to go home," he said. "A third option is to borrow from future time off."

However, companies are also concerned about potential abuse of extended sick leave policies, Sarabacha said. At a recent meeting he attended, an executive at a large financial institution said his organization had done a lot of planning of sick leave policies in the event of a pandemic but isn't going to let employees know out of concern the system could be abused.

3. LACK OF ADEQUATE STAFFING PLANNING

Without a doubt, planning for a scenario in which you lose 40% of your staff for extended periods is difficult. However, there are other staffing scenarios that financial institutions also need to consider if the swine flu strikes hard, experts say.

For example, an organization may see a spike in demand for certain services or products and a sharp drop for others in a pandemic, Zawada said. An insurance company, for instance, might see a decline in property claims but an increase in short-term disability or life insurance claims. If more people stay at home, some financial-services firms expect to see an increased credit card activity. Consequently, a company needs to develop a staffing model that meets customer needs while accounting for staff absenteeism, he said.

"Understanding demand and building appropriate staffing models—many organizations have done it, but some are just beginning," Zawada said.

An area that banks haven't paid enough attention to is succession planning, Gartner's De Lotto said. "People might die or be incapacitated for long periods. How do you arrange for a turnover of command in a department with proper provisioning and passwords when your IT department is sick?"

Permissions could be installed on a thumb drive, but in the end, it's difficult for an organization to imagine large chunks of its managerial staff dead or incapacitated and to plan for successors, he said.

Razook said some banks that have conducted pandemic planning have done a good job at building a skills matrix—conducting an assessment of their employees' skills. That allows them, for instance, to figure out who could fill in as a teller.

"They identify where their issues are and they're cross-training," she said.

4. NOT ACCOUNTING FOR VENDORS

Considering how much most financial institutions are dependent on third-party vendors, a possible pandemic presents hidden risks, said Schneier, the compliance consultant.

"For the minority of institutions that have actionable pandemic plans in place, how many of them are dependent upon their vendors in order for the plan to work? How many of those vendors have their own pandemic response plans in place and how would you even know if those plans are viable?" he said.

"Imagine a likely scenario where there's a quarantine, your staff is sent home to work remotely and one of your key telecom or hosted solution providers has an outage that can't be properly managed because they're operating at severely reduced staff levels. What's your next move?" he added.

Many organizations have tried to assess their vendors' business continuity preparations via questionnaires, but didn't have much success, Zawada said. They either didn't know what to do with questionnaires that were returned or vendors wouldn't cooperate, claiming their plans were proprietary.

"Those that did it well had one-on-one dialogue with their key suppliers and business partners where they may have jointly planned," he said. "They clearly understand each other's business model and expectations. They're working together in a collaborative manner. There is some of that [collaboration] but probably more could be done."

Deloitte's Sarabacha said successful organizations figure out their critical vendors and share as much detail of their pandemic plans as the legal departments will allow in order to gauge how complementary they are. If the plans aren't complementary, then organizations need to consider back up vendors or alternate plans.

The ability to see a vendor's plans—and results of plan testing—starts in the procurement and contract process, he said. More and more organizations are including language in their contracts to cover that oversight, he said: "They're getting more precise in those contracts so you have the right to do it if you choose."

5. NOT TESTING

An area that many financial institutions and other organizations don't focus on enough in their pandemic planning is testing, experts said.

"We can't appraise the effectiveness of our planning until we've triggered the plan - that is, taken action in response to a real situation or in response to well strategized scenario-based testing that examines external factors and incorporates consideration of critical interdependencies," said Carol Ward, an independent banking consultant.

"The complexity and difficulty of setting up scenario-based testing shouldn't be underestimated. Ongoing risk monitoring and testing is the weakest link in the effort to be ready. And I think it is causing the most difficulty," she added.

Since many pandemic plans rely on having workers telecommute, capacity planning is essential, experts said.

"Wouldn't it be terrible to have a plan that says everyone will telecommute and then no one can get into the system?" Razook said. "That's where testing comes in. Have fifty percent [of the workforce] go home and dial into your system and see if it crashes."

Sarabacha said he's seen organizations test whether employees who don't normally work at home can do so, but not test their systems' capacity. "The challenge is from a capacity perspective. Can your internal systems handle the type of load that has never come before?" he said.

Of course, some possible pandemic scenarios are tricky to test. For example, if schools shut down, banks will have employees who need to stay home with their kids—a scenario that's difficult to develop into a tabletop exercise, De Lotto said.

"You can do some remote access tests and table top exercises, but it's kind of hard to simulate this [pandemic]," Zawada said.

Marcia Savage is Feature Editor for Information Security *and Site Editor for SearchFinancialSecurity.com.*

SPAMMERS Take Advantage OF SWINE FLU CONCERN

Bogus messages are a way to trick users and collect email addresses. BY ROBERT WESTERVELT

SYMANTEC CORP. AND SEVERAL OTHER security vendors are tracking a spam wave taking advantage of the swine flu outbreak to trick victims into giving up information or downloading a malicious file.

One of the more serious spam messages contain a malicious PDF file that purports to provide information about the swine flu. If a victim opens the file, their machine is immediately infected with at Trojan that tries to steal sensitive data, said Kevin Haley, director of security response at Symantec. The Trojan, Bloodhound.Exploit.6, was discovered in 2004 and can be detected by most antivirus vendors.

"Protect yourselves and your computer from the human swine that prey on our desire for information to keep us healthy," Haley wrote in the Security Response blog post [http://www.symantec.com/connect/blogs/malicious-code-authors-jump-swine-flu-bandwagon#A268] on malicious code authors jumping on the swine flue bandwagon. "Keep your security software up to date, keep your systems patched, and be suspicious of unsolicited email that talks about topical subjects."

The tactic of using a major event in spam messages has been used incessantly over the years. Spammers have used the Iraq War, the Sept. 11,

2001 terrorist attacks and other global disturbances to trick recipients into reading and clicking on malicious links. Experts say the best defense is to use antivirus, educate end users to avoid opening messages from unknown sources, or at a minimum, that they don't click on the links or open files the messages contain.

The latest swine flu related messages [http://www.symantec.com/connect/blogs/swine-flu-outbreak-headlines-used-spammer-s-gain] also attempt to collect email addresses, possibly for use in future campaigns, noted Mayur Kulkarni of Symantec's email security group in Symantec's Security Response blog.

A sample collected by Symantec found that some messages contained legitimate links to news headlines from reputable news agencies. The spam message links to a form for users to share if they have been personally affected by the flu outbreak, prompting them to give up an email address and phone number.

Security researchers at messaging security vendor Cloudmark Inc. said swine flu related emails spiked almost immediately after news reports about the outbreak in Mexico became public. Messages streamed into more than 20,000 Cloudmark desktop users in one day, the company said.

Romana Ward of UK-based SophosLabs discovered swine flu comment spam messages [http://www.sophos.com/blogs/sophoslabs/v/post/4274] urging members of a Russian pharmaceutical network to sell a cure for the disease. The network sells legitimate generic drugs. The message urges affiliates to add Oseltamivir, a generic form of Tamiflu, to their store catalog. A similar campaign was waged during the bird flu outbreak, Ward said.▸

Robert Westervelt is News Editor for SearchSecurity.com.

TABLE OF CONTENTS

PANDEMIC PREPARATION

PANDEMIC RESPONSE PLANS

FIVE MISTAKES ORGANIZATIONS MAKE

SPAMMERS TAKE ADVANTAGE OF SCARE

TABLE TOP EXERCISE

TECHNOLOGY NEEDS to Be in Place NOW FOR FUTURE EPIDEMICS

Telecommuting is one of the biggest concerns, says U.S. Department of Treasury official. BY TERRY SWEENEY

A LARGE-SCALE FLU EPIDEMIC is a bad time to implement VPNs or work-at-home policies, according to a U.S. Treasury Department official.

The Treasury Department, working in conjunction with the Financial Banking Information Infrastructure Committee (FBIIC), the Financial Services Sector Coordinating Council (FSSCC) and the Securities Industry and Financial Markets Association, tested the business continuity readiness of more than 2,700 participating financial institutions.

The objectives of the exercise, which took place between Sept. 24, and Oct. 12 2007, included getting a clearer understanding of the systemic risks to the financial services sector during a pandemic; improving preparedness by testing pandemic plans; and examining the ripple effects on telecommunications, energy, transportation, IT and other service providers.

On each Monday of the three-week exercise, participants received an email describing simulated infection levels, absentee rates for that period, public health alert levels, food supply levels, and economic data about market activity. The same email contained a link to a questionnaire, where participants assessed the pandemic's impact on business operations and specific departments with employees whose last names began with the letter A, E, F, J, K, N, O, Q, T, U, V, X, Y or Z were presumed absent or sick as part of the simulation. Respondents had two days to discuss their answers internally and then respond anonymously.

Valerie Abend, deputy assistant secretary for critical infrastructure protection and compliance policy at the U.S. Department of Treasury said one area of concern that emerged from the exercise: telecommuting. "If you're not already doing it, it's pretty hard to implement during a crisis. It's an option for our institutions, but many [institutions] haven't really tested their policies," said Abend. "We're not convinced this last mile is going to stand up, even though telecommunications companies have worked hard with the financial services sector."

"Financial services, like healthcare, need a robust last mile—reliable and secure," she added. "And there's a lot of concern there as to whether that can stand up in a pandemic."

Useful or empty exercise?

Safeguarding wealth and protecting markets and financial services companies have been federal government priorities going back at least as far as the superpower nuclear arms race. But emergency response has become more politicized in the post-Katrina era. The SARS outbreak a few years ago, coupled with a potentially virulent avian flu epidemic, have prompted government agencies to work more closely to head off similar situations and criticisms, according to Ken Wilson, president, of Minneapolis-based Wilson Marketing Group Inc., which specializes in pandemic planning and training.

Large companies are more likely to have some sort of pandemic plan in place than medium and small businesses, Wilson said. Small and medium-sized businesses typically "are not prepared, either internally with necessary infrastructure, or on the manpower side," he explained. "What they can do without spending money, they will do. But to get duplicate hardware to support working from home, for

> "[Small and medium-sized businesses typically] are not prepared, either internally with necessary infrastructure, or on the manpower side."
>
> –KEN WILSON, president, Wilson Marketing Group Inc.

History of Pandemics

Influenza pandemics are rare but have typically occurred every 10 to 50 years throughout recorded history. There were three in the last century:

1918

Spanish flu–The most devastating flu pandemic in recent history, killing more than 500,000 people in the U.S., and 20 million to 50 million worldwide.

1957-58

Asian flu–First identified in China, this virus caused roughly 70,000 deaths in the U.S. between 1957 and 1958.

1968-69

Hong Kong flu–First detected in Hong Kong, caused roughly 34,000 deaths in the U.S. from 1968 to 1969. H3N2 viruses still circulate.

–COMPILED BY MARCIA SAVAGE

example, is another question."

Perhaps an even more troubling issue is the likelihood that many firms are unaware of how critical it is to prepare well in advance of a pandemic. "We have not given any thought to this. Not sure that is a good answer, but [there are] only so many 'disasters' we can manage at once," said the CTO of a major ecommerce site, who asked not to be identified. "We are greatly expanding our remote capacity for business reasons and a side benefit will be [being] better able to address an issue like this."

In industry sectors like financial services, there are government advisories [http://www.federalreserve.gov/newsevents/press/bcreg/20060315a.htm] to have some sort of pandemic plan. But industry itself has also become a bit of an enforcer, according to Wilson.

"A lot of large companies are going into their supply chain and saying 'If you want to remain a viable supplier to us, demonstrate that your pandemic plan will work.' So some companies are being forced to do pandemic planning, whether they like it or not." ›

Terry Sweeney is a Los Angeles-based freelance writer and editor, and has covered IT, security and networking for more than 20 years. He can be reached at terry@tsweeney.com.

TECHTARGET SECURITY MEDIA GROUP

INFORMATION SECURITY®

EDITORIAL DIRECTOR Kelley Damore

EDITOR Michael S. Mimoso

SENIOR TECHNOLOGY EDITOR Neil Roiter

FEATURES EDITOR Marcia Savage

ART & DESIGN
CREATIVE DIRECTOR Maureen Joyce

COLUMNISTS
Jay G. Heiser, Marcus Ranum, Bruce Schneier

CONTRIBUTING EDITORS
Michael Cobb, Eric Cole, James C. Foster, Shon Harris, Richard Mackey Jr., Lisa Phifer, Ed Skoudis, Joel Snyder

TECHNICAL EDITORS
Greg Balaze, Brad Causey, Mike Chapple, Peter Giannacopoulos, Brent Huston, Phoram Mehta, Sandra Kay Miller, Gary Moser, David Strom, Steve Weil, Harris Weisman

USER ADVISORY BOARD
Edward Amoroso, AT&T
Anish Bhimani, JPMorgan Chase
Larry L. Brock, DuPont
Dave Dittrich
Ernie Hayden, Seattle City Light
Patrick Heim, Kaiser Permanente
Dan Houser, Cardinal Health
Patricia Myers, Williams-Sonoma
Ron Woerner, TD Ameritrade

SEARCHSECURITY.COM
SENIOR SITE EDITOR Eric Parizo

NEWS EDITOR Robert Westervelt

ASSOCIATE EDITOR William Hurley

ASSISTANT EDITOR Maggie Wright

ASSISTANT EDITOR Carolyn Gibney

INFORMATION SECURITY DECISIONS
GENERAL MANAGER OF EVENTS Amy Cleary

EDITORIAL EVENTS MANAGER Karen Bagley

VICE PRESIDENT AND GROUP PUBLISHER
Doug Olender

PUBLISHER Josh Garland

DIRECTOR OF PRODUCT MANAGEMENT
Susan Shaver

DIRECTOR OF MARKETING Kristin Hadley

SALES MANAGER, EAST Zemira DelVecchio

SALES MANAGER, WEST Dara Such

CIRCULATION MANAGER Kate Sullivan

ASSOCIATE PROJECT MANAGER
Suzanne Jackson

PRODUCT MANAGEMENT & MARKETING
Corey Strader, Jennifer Labelle, Andrew McHugh

SALES REPRESENTATIVES
Eric Belcher ebelcher@techtarget.com

Neil Dhanowa ndhanowa@techtarget.com

Patrick Eichmann peichmann@techtarget.com

Jason Olson jolson@techtarget.com

Jeff Tonello jtonello@techtarget.com

Nikki Wise nwise@techtarget.com

TECHTARGET INC.
CHIEF EXECUTIVE OFFICER Greg Strakosch

PRESIDENT Don Hawk

EXECUTIVE VICE PRESIDENT Kevin Beam

CHIEF FINANCIAL OFFICER Eric Sockol

EUROPEAN DISTRIBUTION
Parkway Gordon Phone 44-1491-875-386
www.parkway.co.uk

LIST RENTAL SERVICES
Kelly Weinhold
Phone 781-657-1691 Fax 781-657-1100

REPRINTS
FosteReprints Rhonda Brown
Phone 866-879-9144 x194
rbrown@fostereprints.com

TechTarget
The Technology Media ROI Experts

INFORMATION SECURITY (ISSN 1096-8903) is published monthly with a combined July/Aug., Dec./Jan. issue by TechTarget, 117 Kendrick St., Suite 800, Needham, MA 02494 U.S.A.; Phone 781-657-1000; Fax 781-657-1100.