international response. Such moves gave other nations a head start in reinforcing surveillance efforts and trying to slow the initial spread of the virus to win time for a vaccine to be prepared.

More waves of H1N1 flu will come, but its health impact will diminish as more people obtain natural immunity. Public-health officials around the globe can take some comfort in the fact that, for now, the virus seems less deadly than they had feared. They can also take pride in having struck a good balance between uncertainty, taking action and minimizing economic impacts and social disruption.

Informing the public about the nature and severity of the disease was a tremendous challenge — especially when it came to explaining the uncertainties surrounding the severity, epidemiology and pathology of the virus. In the United States, the initial communications were overseen in large part by Richard Besser, acting director of the CDC at the time (see page 150). It was a challenge he and the agency rose to admirably. The news media and flu bloggers also generally responded well. Despite their well-known fascination with worse-case scenarios, mainstream news outlets for the most part did a good job of not sensationalizing the threat, and of debunking individuals and organizations looking to sow unfounded doubts about vaccine safety and the necessity of a robust public-health response.

Unfortunately, official efforts to build trust in the pandemic response were not helped by overly optimistic predictions of how much and how quickly vaccines would be available. This underscores a significant technological deficiency: the reliance on a small number of suppliers, with almost all vaccines made by growing the virus in eggs, a process that takes around six months to get shots into production. The spread of H1N1 flu around the world in a matter of weeks highlights the need to develop novel vaccines, which would a provide quicker turnaround, and for government incentives to encourage manufacturers to move away from egg-based production.

Analysis of the H1N1 virus suggests that this new strain had been circulating in pigs for almost a decade, and probably jumped to humans months before it was detected in Mexico. That it was not spotted earlier is unacceptable. Public- and animal-health communities need to help increase surveillance for emerging diseases with pandemic potential.

The danger now is that last year's relatively mild pandemic will create a false sense of security and complacency. The reality is that next time we might not be so lucky — especially given that this time most of the world's population, living as they do in developing countries, had no access to either vaccines or antiviral drugs. Governments and scientists would do well to redouble efforts to reinforce our pandemic defences, and to draw what lessons they can from this outbreak as a dry run for a more severe pandemic. ■

# Security ethics

## Manufacturers of computer systems should welcome researchers' efforts to find flaws.

In late December, Berlin-based computer-security researcher Karsten Nohl announced that his group had found a vulnerability in the algorithm used to prevent eavesdropping in the most widely used mobile telephone standard in the world.

News outlets around the globe quickly reported that the research would make it easy for anyone to listen in on mobile telephone calls. The industry group that promotes the standard, the GSM Association, just as quickly defended the system and played down the importance of Nohl's finding.

The episode has highlighted an ongoing tension in computer-security research. The need for such research has never been higher: malicious hacking attacks are rapidly getting bolder and more sophisticated, even as law-abiding citizens are being asked to do everything from vote to have their medical information stored on computerized systems. The best way for researchers to improve the security of these systems is to attack them — to find their flaws so that they can be fixed. But this can lead researchers into a grey area in which their efforts can look a lot like criminal activity.

Some manufacturers, fearful that the revelation of a flaw could undermine their credibility in the marketplace, have reacted furiously to such research. In 2008, for example, two groups were the subject of legal action by organizations attempting to prevent the release of weaknesses the researchers had found in the smart cards used in mass transit systems (see *Nature* doi:10.1038/news.2008.1044; 2008).

Both those attempts were ultimately unsuccessful and the research was disseminated. Nonetheless, the threat of legal action haunts the field, not least because of uncertainty over exactly what work is legal. Researchers were particularly incensed about the 2008 cases because both the groups had followed the community's widely accepted 'responsible disclosure' protocol: researchers who uncover a flaw don't go public until the system's developer has had a chance to fix it.

They were right to be outraged: security research done in the spirit of responsible disclosure is something that computer-system manufacturers should encourage, not fight. When flaws are detected and fixed before outlaws can exploit them, everyone benefits.

That said, not every computer-security researcher has been as meticulous about the conduct of their work. Investigators say that they have seen work published or presented at conferences that they personally are uncomfortable with.

The computer-security community should engage in a wide-ranging discussion of the ethics of its work, especially as researchers move into ever greyer areas, such as examining or even controlling networks of computers that have been taken over by criminals. If nothing else, this discussion could help it to head off a worst-case scenario in which a research project that oversteps the bounds leads to an onerous crackdown that impedes genuinely useful research.

Computer-security research is a relatively young field and many of its leading members are far removed from the traditional image of academics. Much of their research is disseminated through less formal routes than peer-reviewed journals, such as blogs, and their conferences can seem like strange, anarchistic affairs to researchers in other fields.

But the public now relies on these people to defend it against everything from credit-card fraudsters to terrorists. They are genuine researchers. And they deserve a considered ethical framework within which to conduct their vital activity. ■