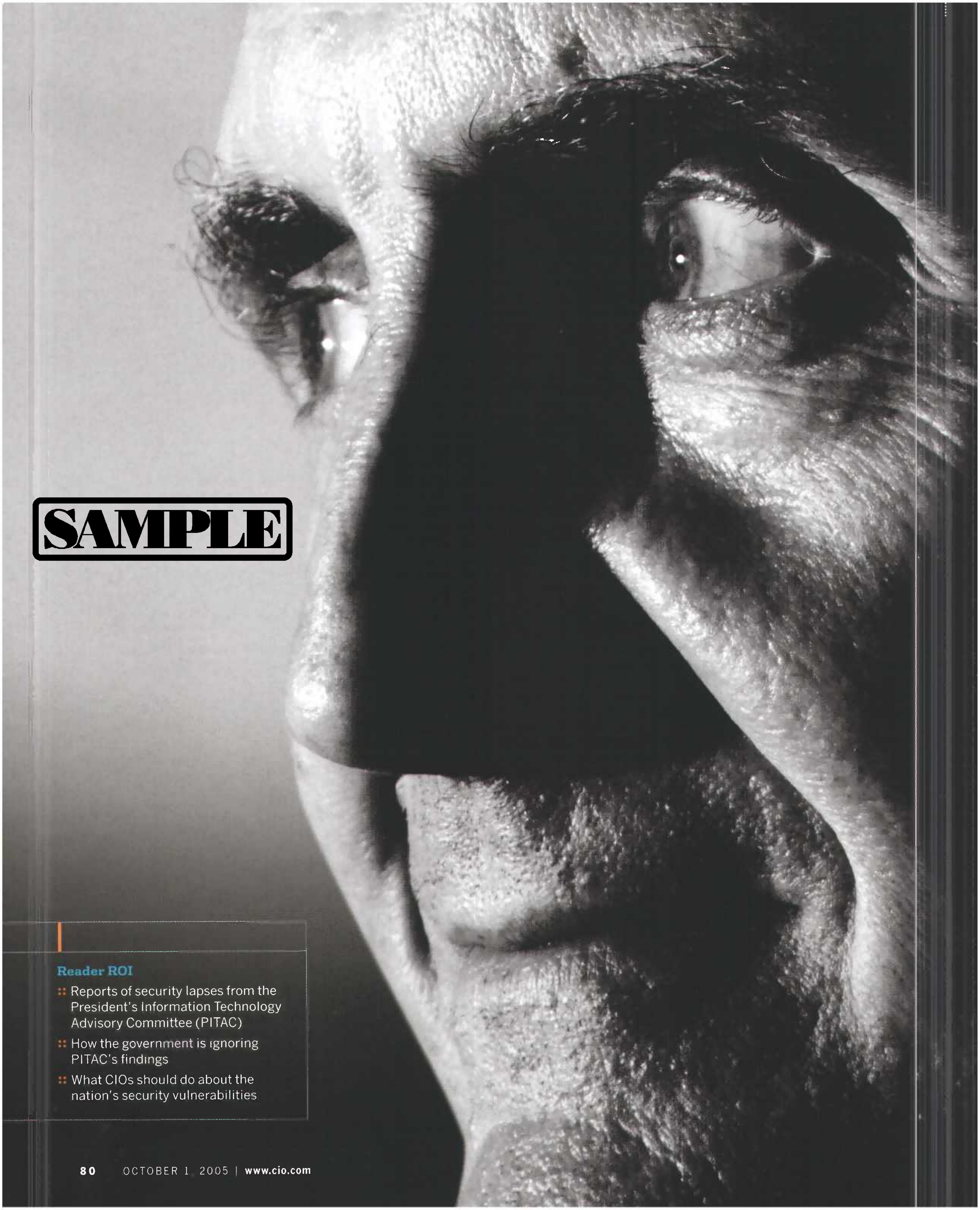


Reader ROI

- Reports of security lapses from the President's Information Technology Advisory Committee (PITAC)
- How the government is ignoring PITAC's findings
- What CIOs should do about the nation's security vulnerabilities

Ed Lazowska, cochairman of the President's Information Technology Advisory Committee, says that **there is a looming security crisis**, and the government, vendors and CIOs aren't doing enough to stop it

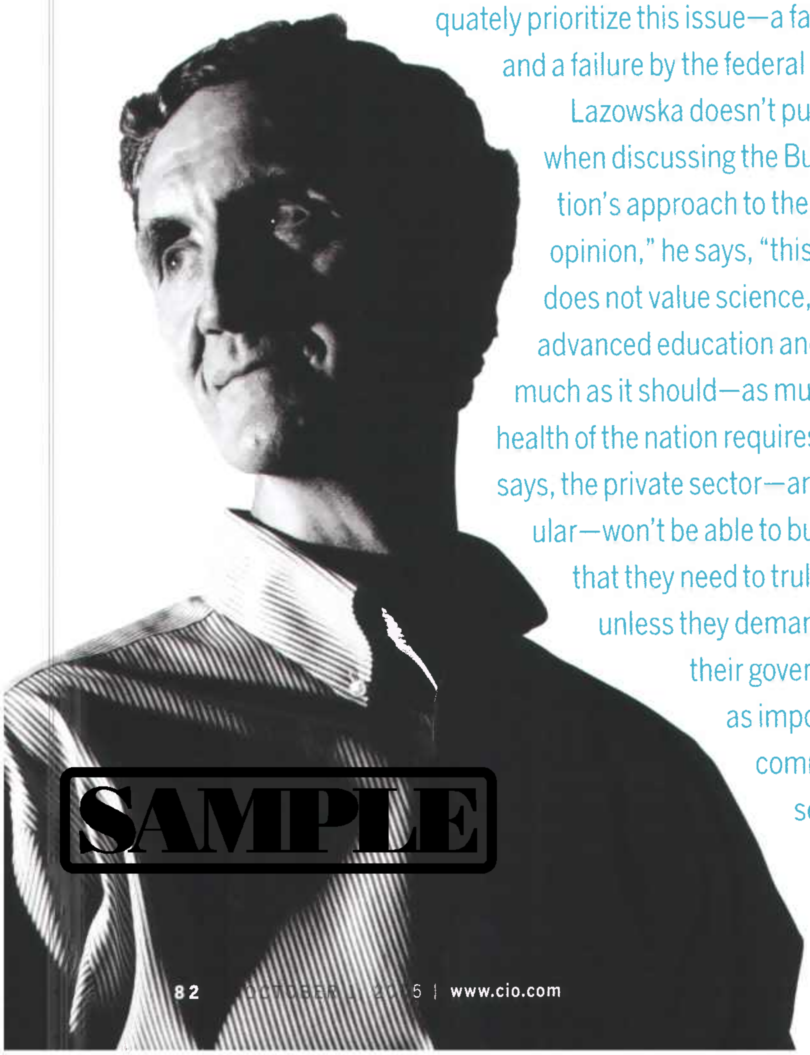
The Sky Really Is Falling

BY BEN WORTHE

PHOTOGRAPHY BY BRIAN SMALE

Ed Lazowska holds the Bill & Melinda Gates Chair in Computer Science & Engineering at the University of Washington, where he specializes in the design, implementation and analysis of high-performance computing and communication systems. In May 2003, President Bush appointed him cochairman of the president's Information Technology Advisory Committee (PITAC) from 2003 to 2005. PITAC, created by an act of Congress in 1991, is made up of experts from both academia and the private sector who advise the President on IT issues. It has traditionally been one of the most important mechanisms that the government has to ensure that the nation's R&D programs have the appropriate scope and direction to keep the country at the forefront of the IT industry. Under Lazowska's leadership, PITAC studied three issues: IT for health care, the future of computational science and cybersecurity. PITAC's report on cybersecurity, called "Cyber Security: A Crisis of Prioritization," was published in February. "The title nicely summarizes our findings," says Lazowska. "There is a crisis, and it is due to a failure to adequately prioritize this issue—a failure by CIOs, and a failure by the federal government."

Lazowska doesn't pull any punches when discussing the Bush administration's approach to the issue. "In my opinion," he says, "this administration does not value science, engineering, advanced education and research as much as it should—as much as the future health of the nation requires." As a result, he says, the private sector—and CIOs in particular—won't be able to buy the products that they need to truly be secure unless they demand more from their government and, just as importantly, show a commitment to cybersecurity by paying for state of the art products.



CIO: You're not very optimistic about the state of U.S. cybersecurity. What is the one-minute version of the problem?

Ed Lazowska: There is a big gap between what we already know about cybersecurity and our deployment of technologies and processes to improve it. That's a CIO problem. There's also a big gap between what we already know about cybersecurity and what we need to know in order to engineer adequately secure systems for the long-term future. That's a federal government problem, because the federal government is responsible for R&D that looks out more than one product cycle—R&D such as engineering a more secure version of the Internet (see "Blame the Internet," Page 84).

In your report to the president, you concluded that IT infrastructure is highly vulnerable. What are some of the key vulnerabilities?

We see some of the effects of cybervulnerabilities on a daily basis on the front page of our newspapers: phishing attacks, pharming attacks, denial-of-service attacks and large-scale disclosure of credit card information. Even phishing attacks, which seem easy to dismiss as a gullibility problem, arise from the basic design of the protocols we use today, which make it impossible to determine the source of a network communication with certainty.

The public, and most CIOs, do not see many activities that are even more threatening. The nation's IT infrastructure is now central to the life of all other elements of the nation's critical infrastructure: the electric power grid, the air traffic control network, the financial system and so on. If you wanted to go after the electric power grid—even the physical elements of the electric power grid—then a cyberattack would surely be the most effective method. It's also worth

National Security Crisis

The nation faces a looming security disaster. That's one of the findings of a report from the **President's Information Technology Advisory Committee**, which was cochaired by Ed Lazowska and which details the vulnerabilities of our IT infrastructure. For a link to this report, go to **www.cio.com/100105**.

noting that the vast majority of the military's hardware and software comes from commercial vendors. PITAC was told that 85 percent of the computing equipment used in Iraq was straight commercial. So the military itself is arguably about as vulnerable to a cyberattack as the civilian sector.

Some of the problems, such as software not being designed with security in mind, indicate that CIOs are somehow complicit. In your opinion, are CIOs victims or are they part of the problem?

The answer surely is both. CIOs are partially responsible for the insecure state of today's operating systems, because they failed to see the handwriting on the wall and prioritize security. Vendors produce what we are willing to purchase. CIOs are largely responsible for the failure of their organizations to operate at the current state of the art with respect to cybersecurity, and very few organizations operate at the current state of the art.

Now, the problem is that you can't suddenly decide that you want something like security and expect to be able to buy it, because the technology doesn't necessarily exist. Almost no IT company looks ahead more than one or two product cycles. And historically in IT, those ideas comes from research programs that the federal government underwrites. Just think about e-commerce: You need the Internet, Web browsers, encryption for secure credit card transactions and a high-performance database for back-end systems. The ideas that underlie all of these can trace their roots to federally funded R&D programs.

That's how this relates to the R&D agenda. Long-range R&D has always been the role of the national government. And the trend, despite repeated denials from the White House to the Department of Defense, has decreased funding for R&D. And of the R&D that does get funded, more and more of it is on the development side as opposed to longer-range research, which is where the big payoffs are in the long term. That's a more fundamental problem that CIOs aren't responsible for.

You feel strongly that the government's treatment of cybersecurity R&D has been particularly neglectful.

PITAC found that the government is currently failing to fulfill this responsibility. (The word *failing* was edited out of our report, but it was the committee's finding.) Let me talk very quickly about three federal agencies that you might think are focusing on this but are not:

» Most egregiously, the Department of Homeland Security simply doesn't get cybersecurity. DHS has a science and technology (S&T) budget of more than a billion dollars annually. Of this, [only] $18 million is devoted to cybersecurity. For FY06, DHS's S&T budget is slated to go up by more than $200 million, but the allocation to cybersecurity will decrease to $17 million! It's also worth noting that across DHS's entire S&T budget, only about 10 percent is allocated to anything that might reasonably be called "research" rather than "deployment."

» Defense Advanced Research Projects Agency (DARPA) is investing in cybersecurity, but has classified all of its recent new program starts in this field. It's fine to do classified research, but we must also recognize the negative consequences, and we should (but don't) fund nonclassified research to make up for it. One negative consequence is that classified research is very slow to impact commercial IT systems, on which the entire nation, and even much of the Department of Defense, relies. Another negative consequence is that the nation's university-based researchers cannot participate, because universities do not perform classified research. This eliminates many of the nation's best cybersecurity researchers. It also means that students are not trained in cybersecurity—the training of students is an important byproduct of research.

» The National Science Foundation (NSF), in FY04, mounted a new cybersecurity research program, which was able to fund only 8 percent of the proposals it received. PITAC recommended immediately adding $90 million annually to the NSF Cyber Trust program, as a start. Thus far, there is no sign of any action on this recommendation.

Where would this $90 million come from?
The federal budget is trillions of dollars, and we waste billions every month. This nation makes all kinds of large-scale spending decisions, and $90 million is one umpteenth of one umpteenth of 1 percent. And the question is, is cybersecurity worth it to this nation?

What are some of the things that more research might yield?
Cybersecurity, today, is all about securing the perimeter, but there is really no "inside" and "outside" anymore. This is not an argument against firewalls, intrusion detection systems and the like. Rather, it is a very strong argument against placing complete faith in them. Today, in cybersecurity, we are applying Band-Aids, and we are developing the next generation of Band-Aids, but we are not investing in research programs that will yield fundamentally new system architectures that will meet the challenges we face today and will face in the future. We need to develop both static and dynamic analysis tools that detect vulnerabilities. We need programming languages that include fundamental security features. We need techniques for assembling trusted software systems out of multiple components.

Also, interface design is a very significant issue that receives far too little attention. The problem is lousy software designs and lousy human interfaces, on systems ranging from the routers that control the nation's Internet to the dialog boxes that your browser presents. A few years ago, researchers from Princeton and the University of Washington conducted a study of what users actually comprehend when they read these dialog boxes, and the answer, not surprisingly, is that users don't have a clue what these dialog boxes are trying to tell them. This is absolutely not a user problem! Of course, it turns out that a large proportion of Internet routing errors are happening for just this reason—someone in an ISP changes the configuration of some routers and an error is introduced. But it also turns out that the configuration interface on many Internet routers is incredibly primitive, and thus hugely error-prone.

Is there a role for the private sector and in particular CIOs when it comes to seeing some of these changes enacted?
CIOs and CEOs must insist on different behavior by the current administration. Our nation's health and security depends on it. On their own, CIOs—that is, the private sector—must install and operate systems that match the state of the art in terms of cybersecurity. CIOs must demand that software vendors design and correctly implement these systems, and most importantly, CIOs must be willing to pay for it. Also, many corporations now have a chief information security officer, which is an important step. And there is an increasing trend toward having a person with IT qualifications on the corporate board of directors, just as a person with appropriate financial experience must be a board member in order to chair the audit committee. These sorts of things are becoming the standard of practice, and corporations that fail to meet this standard of practice will do so at their own jeopardy.

E-mail feedback on this article to Senior Writer Ben Worthen at *bworthen@cio.com*.

Blame the Internet

The Internet wasn't made for today's commercial traffic—should it be rebuilt?

Ed Lazowska believes that there's a single culprit at the heart of many of today's cybersecurity problems: the Internet. When it first started carrying packets more than 35 years ago, the Internet was little more than a research project. Since then, it has evolved into the commercial phenomenon on which we all rely. But the technology on which the Internet is built, TCP/IP, and other switching and routing protocols, weren't created with modern usage and its associated modern security needs in mind. "We are asking the Internet to handle a load and perform tasks that it wasn't designed for," Lazowska says. "The fact that it has been able to do so is remarkable. It is no surprise at all that it isn't perfect for today's environment."

Patches and updates won't solve this problem. "Many of the protocols that we use are inherently insecure," Lazowska says. "They can't be made more secure by evolution. They need to be rethought." Unfortunately, the only solution is replacing the Internet with something new, just like CIOs have to replace old Cobol systems that wear out.

The entire Internet was actually replaced once before in the early 1980s when the whole Internet switched over to TCP/IP on one pre-arranged day. Back then there were only about 1,000 computers connected to the network, however. Today, says Lazowska, "It will be a big, expensive, worldwide job. The United States does not currently have a plan for switching to a more secure and more reliable Internet, but it needs to have one," he says, "because the cost of not doing it is too great." *–B.W.*