THE NEW ATLANTIS
A JOURNAL OF TECHNOLOGY & SOCIETY

*Q&A*

# Is Cyberspace Secure?

## *An Interview with Howard A. Schmidt*

*Howard A. Schmidt has spent his career on the cutting edge of computer security. A specialist in computer forensics, he has worked for the FBI and the Air Force, where he established the federal government's first dedicated computer forensics laboratory. Microsoft hired him in 1997, and he served as the company's Chief Security Officer during the period when cybersecurity became a broadly recognized priority for both government and private industry.*

*Shortly after the September 11 attacks, Mr. Schmidt returned to government service as vice chairman of the White House's Critical Infrastructure Protection Board, an organization formed to coordinate the work of government agencies on aspects of critical infrastructure—especially information systems. When the board's chairman, Richard Clarke, resigned in early 2003, Mr. Schmidt replaced him as the government's "cybersecurity czar."*

*The board's first (and only) major publication—the "National Strategy to Secure Cyberspace"—was released in February 2003. The report lays out a general cybersecurity plan, making broad policy recommendations for both the public and the private sectors. The new Department of Homeland Security (DHS) will play a central role in the strategy, serving "as the primary federal point-of-contact for state and local governments, the private sector, and the American people" on cybersecurity issues. DHS is absorbing several agencies that handle cyberspace, including the White House board (now formally dissolved by executive order) that Schmidt has been heading.*

*On March 6, 2003, just a few weeks after the release of the new cybersecurity strategy, we sat down with Howard Schmidt in his office.*

~

**The New Atlantis:** How would you define the term "cybersecurity" for laymen?

**Howard Schmidt:** For the layman, cybersecurity is the realization that computer systems affect our basic needs on a daily basis. Electricity, water, telephone—these things are all run by computers, and my job is to work with owners and operators and government agencies to make sure that they continue to function properly and are not disrupted because of security events that then, in turn, affect our daily lives.

**NA:** How does cybersecurity relate to other areas of critical infrastructure—to energy, food, transportation, finance, and so forth?

**HS:** We've received tremendous benefit from the IT revolution, and as a result we've been able to do things we've never been able to do before. It is the under-

pinning of all those utilities, all those critical infrastructures that you mentioned. But there are also new risks. For example, if a computer system is down for the national rail system, you could still physically move trains, but you wouldn't want to, because you won't know where perishable items are supposed to be delivered. Or perhaps chemicals that need to be moved to help water treatment plants won't get there—so within a matter of time, water treatment facilities would be having problems. The underpinning of all these critical infrastructures are computers that must be protected.

**NA:** Looking through the cyberspace strategy your office just published, this was the closest thing we could find to a description of a specific threat:

> In peacetime America's enemies may conduct espionage on our Government, university research centers, and private companies. They may also seek to prepare for cyber strikes during a confrontation by mapping U.S. information systems, identifying key targets, lacing our infrastructure with back doors and other means of access. In wartime or crisis, adversaries may seek to intimidate the nation's political leaders by attacking critical infrastructures and key economic functions or eroding public confidence in information systems.

Could you expound on that a little? Could you offer other examples, other specific threats to cyberspace?

**HS:** This is the high-level perspective on the worst things that could happen if we don't continue to develop more robust cybersecurity. Let me qualify some of these things, when we talk about threats. Take the recent Slammer worm that took place a little over a month ago, for instance. When that happened, we did not get the kind of notice you have when you see a smoke plume coming off the trailing edge of a rocket saying, "Boy, there's a threat." Nor did we see some underground communication that said, "We're going to do this specific act against these specific systems."

So identification of threats in more specific terms than we've outlined in the strategy is oftentimes a challenge. We know they exist. We've seen them by virtue of the disruptions they cause—everything from the Morris worm years ago to the Melissa macro virus, to Slammer, Code Red, NIMDA, the attacks on DNS servers. We know the threats are out there, we've seen them occur. But in many cases, we don't know what the sources are, and that's a challenge we've got. So to get more detailed as to what the threats are, I think, is to do nothing more than look at what has hit us so far, and take those disruptions very seriously.

**NA:** Some people have argued that the threat to cybersecurity has been somewhat inflated—for example, that the effects of the recent Slammer/Sapphire worm were exaggerated. You've probably seen some of that criticism in response to the new cybersecurity strategy.

**HS:** I don't think the threat is inflated at all. The perceived impact of some

threats, like the Slammer worm, depends a lot on inaccurate reporting. As time goes by, we have the ability to better identify what the true effects were. That doesn't change the threat model, though. Part of the reason this activity was not more disruptive is that we have been paying attention to cybersecurity over the past two years. My response to those critics who say "it's overinflated" or "it's done to create FUD [fear, uncertainty, and doubt] and scare-mongering" is that the more we become dependent upon IT systems, the more we depend on the critical infrastructure being run by IT systems, the harder we'll have to work to make sure we don't fall into the situation where these threats become more than just an inconvenience.

**NA:** Your predecessor Richard Clarke famously spoke about a "digital Pearl Harbor," a phrase that has been very harshly criticized in some quarters, especially after September 11. Many people argued that it was inappropriate to compare threats in cyberspace to threats against civilian or military targets in the offline world. What's your feeling about the term and the concept of a "digital Pearl Harbor"?

**HS:** The term "digital Pearl Harbor" was actually used years ago in one of the early information warfare settings, in one of the hearings that were going on up on the Hill. It's been used over and over again, to make a point about a surprise attack, a debilitating attack. It's unfortunate that a description that is put out there with the best intention gets misinterpreted as being something more than it is.

Part of the reason that a "digital Pearl Harbor" hasn't occurred is because we've been talking about cybersecurity. Something similar happened with the Y2K issue: Y2K didn't happen because we talked about it, we were prepared for it. So we need to continue our preparedness, we need to continue to champion cybersecurity. We can enjoy the features, the richness, the robustness of IT, and protect privacy while still being secure. But I don't use that term because I think it has become a distraction.

**NA:** What about the term "cyberterrorism"? Both you and Mr. Clarke are opposed to it, and the term doesn't appear at all in the cybersecurity report. Can you explain why?

**HS:** Well, for one thing, it conjures up physical events that would not actually be taking place in cyberspace. The word "terrorism" has connotations—like mass panic—which I don't think you would see in the cyber-world. So instead we talk about cybersecurity, and the threats against it, and the integrity and availability of systems.

**NA:** But if terrorists were to use the Internet in a way that would, say, incite mass panic, then that might be an acceptable use of the term.

**HS:** I think if we ever saw that occur, or if we ever saw indications that that was a way people were looking to do business in the terrorism world, then yes, we may actually be able to use that term for that specific event. Most of what we see, most disruptions, we don't know in many cases whether it's coming from the Middle East or the Midwest. But the fact that it's disruptive is what concerns us.

**NA:** Let's return to the new cybersecurity strategy. According to a recent article in *Slate*, "The bulk of the report's solutions are lame. Most are meaningless jargon, such as suggesting that 'future components of the cyber-infrastructure are built to be inherently secure and dependable for their users.' A fantastic sentiment, but as mushy as stating that the president is 'for the children.'" How would you respond?

**HS:** Obviously we didn't think it was a lame report. We thought it was a serious and well-balanced report. We had input from a widespread number of people: industry, academia, government, security consultants, IT vendors—and basically, when you read through the report, everybody is committed to being more secure. I think the better question that some of these critics should be asking is: "Why don't we stop the criminals from doing these things?" It would be very nice not to have to worry about that—to receive the rich, robust features we have without worrying about somebody violating your system because of a flaw that wasn't built intentionally. In the meantime, let's make sure that the people that are committing the felonies, the criminal acts, abusing the software—let's make sure that there's attribution.

**NA:** In the new cyberspace strategy, many responsibilities will be shifting to the Department of Homeland Security. The intention is to evolve from existing organizations in the private sector and existing government agencies to create a more effective cybersecurity system. But how long will it take DHS to get a handle on these things? Will a "national cyberspace security response system" be up and running in a year? Two years?

**HS:** One of the things relative to DHS when it comes to cyberspace is that many key institutions are already in place. The National Communications System, the National Infrastructure Protection Center (NIPC) within the FBI, the Federal Computer Incident Response Center within GSA, the Department of Energy Information Assurance Division and the Critical Infrastructure Assurance Office—these are all organizations that have been independently functioning in this area for at least a couple of years now. Consequently, the ramp-up time is going to be much shorter.

For example, consider the National Cyberspace Security Response System, an idea that we propose in the report. The government—in this case, the National Communications System (NCS) has had the lead on it—has been building out the

Cyber Warning Information Network (CWIN), expanding that into the private sector, so when they start seeing an incident take place they have the ability to react.

At the same time, the FBI has been building relationships with the Information Sharing and Analysis Centers (ISAC) to do a similar thing. What we do now is collapse them together and we'll have the capabilities a lot quicker than we had anticipated.

Some of the first challenges are just the physical facilities and just getting these things put together. But the move to DHS shouldn't impact our current status in any way, shape or form, and the reorganization will do nothing but enhance it in the long term. I would be seriously surprised if, within a year, we're not beyond full operating capacity, with a new system up here that runs as flawlessly as ever. They've got some really good people over there who have been doing this for a while.

**NA:** You have an unusual personal history, having gone back and forth between the public sector and private sector on these issues. How would you respond to the security critics who say that the private sector has a poor attitude when it comes to cybersecurity? Most prominently, there's the fear of embarrassment, the risk of tarnishing the company's reputation if it reveals security flaws.

**HS:** Let me break that into two separate pieces. The first piece is the private sector identifying vulnerabilities and communicating aspects of that vulnerability; the second piece is when companies themselves become victims.

First, on the vulnerabilities. Yes, there used to be a time when many companies practiced "security by obscurity." The concept was, "Well, we know about the vulnerability, probably nobody else knows about it, there's no rush to get this fixed." Once again, as the threat picture has changed over time, as we've become more dependent on IT infrastructures and Internet Protocol-based networks, we've seen that change dramatically. Many people—and I used to be one of them, when I was with the government before—thought that if there was a vulnerability, they wanted to know about it. And what happens is, if a lot of people know about it, the exploit comes before the fix does. Many times, that just makes things worse.

So you have to look at it from a balanced vulnerability-reporting perspective. No company has a program that says, "Oh, we're not going to worry about it." Many of them have set up teams that work nonstop on critical vulnerabilities, to get the work started on the patches right away and to get them out to consumers. So I don't think you'll see companies just knowingly letting things sit in the background and hoping nobody finds out about it.

Second, on being the victims. There's always a sense, if something bad happens,

that you are at fault. I don't know many people who'd like to raise their hands and say, "I've failed today." So consequently, they may not want to report it internally. They will often just try to fix it and move on, which doesn't give us good data on what is really going on out there.

At the same time, the law enforcement agencies that collect this information have changed the way they do business. They're very, very circumspect about making a big issue out of a vulnerability because of the fear of harming the companies. So we're working more closely together; we still have a long way to go; we still need to make it less shameful to be a victim—and clearly, that's the point: you're a victim.

**NA:** Some people argue that, by allowing vulnerabilities and victimization to stay more secret—which is what the FBI and other investigative agencies are trying to do, so that companies will feel encouraged to come forward—that some of the negative information that should be getting to investors just isn't reaching them.

**HS:** It's a tough trade-off. The other piece that plays into this is deterrence. If you don't see people being arrested and successfully prosecuted, there is this perception that they're getting away with it, when in reality they're not.

Relative to investors: Any of us who have been in security for any amount of time have a saying that we use over and over again: "Security is not a destination, it's a journey." So if there is a gaping security vulnerability that has allowed something to happen for a period of time, I can guarantee that vulnerability will soon be fixed. Is this something that needs to go to the investor community, because it was a problem that occurred at one point in time? That's for the board of directors and the company principals to decide, working with the investors.

**NA:** There are also cybersecurity problems at the end-user side, the individual side. How do we go about creating an awareness of cybersecurity, a culture of cybersecurity? Especially among ordinary individuals—for example, people who unthinkingly use one password for everything—how do you make them aware of the risks, aware of issues like identity theft?

**HS:** Clearly, there are some people who aren't aware of the risks. Some people think that they're only one of 70 million users, so they feel statistically safe. And then there are the folks who say, "Yeah, I know I'm probably not going to be safe, but it's just too hard to remember all these passwords," which brings us back to the technological fix: for example, two-factor authentication, with smartcards or biometrics.

How do we do more on education? First, the Federal Trade Commission has launched its "Safe at Any Speed" program, designed for consumers and small-to-medium enterprises. It's online; that information is out there.

Second, we have been working with the National Cyber Security Alliance, which includes both government agencies and private sector companies. We have a website that consumers can visit to see not only the risks, but also some FAQs on anti-virus software and why you really need it, personal firewalls, and use of broadband technology. So that's a component that we have right now.

Another thing that we're working towards is drawing enough resources together to do some public service announcements on television, which reaches a much broader audience. We also have a program that's run through the National Infrastructure Protection Center (NIPC) and System Administration, Networking, and Security Institute (SANS) to try to raise awareness in the school systems. It has a double effect: first, the kids get energized about submitting posters and everything else, and the teachers become more aware of the issues. We've also been working with the American Association of Community Colleges, EDUCAUSE, and the universities.

**NA:** What is the official government position on so-called "patriotic hacking"—that is, people sympathetic to the United States, who would deface websites or otherwise use their computer skills against "enemy computers," say, in conjunction with a U.S. military attack on Iraq.

**HS:** NIPC sent out a clear message a few weeks ago saying that this kind of thing cannot be condoned, that it is not an official action, that it is a felony and people will be prosecuted if they do that.

**NA:** How do other countries compare to the U.S. in the area of cybersecurity—in terms of both capability and interest?

**HS:** I think the interest is high in many international venues. I was just over in the U.K. not too long ago. The U.K. has set up a couple of offices similar to ours—high-level government offices to coordinate cybersecurity activities. Canada has the Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP). Australia has its own system, as does Germany. So we're seeing a lot of interest.

As far as capabilities, it varies once again from country to country, based on their dependency on IT infrastructure. As that dependency continues to increase, their cybersecurity capabilities have to be more robust. That's one of the things that we've been working on with them.

There's good news here. We were already a long way down the path of dependency on IT systems when the security issues started to pop up and started to become viable and relevant. Since many other countries are not quite as dependent as we are, they have the ability to get ahead of the cybersecurity game sooner, relatively speaking, than we did.

**NA:** What would you say have been the greatest successes to date of the public-private partnership on cybersecurity?

**HS:** First and foremost, this has become a CEO issue. For those of us who have been in the security business, one of the things we've always lamented is, "Well, we can't get the boss's attention on this." The boss is now paying attention.

The second success is that we've raised awareness levels. After we released the draft national strategy in September 2002, a number of different sectors came forth with their strategies at the same time. Different sectors came out saying, "Here's what our strategy is. Here's how we're going to achieve better security. Here's how we're going to shore up national security, law enforcement, public safety, and economic prosperity."

And third—and I receive a tremendous amount of enjoyment from this—are the actual changes that have taken place as a result of this growing awareness. You have people deploying security strategies, but also people doing more to build security into product implementation in the first place. Industry has responded. We just have to keep the message going: we want the features, but we want the security to go along with it.