



Cyber 9/11

How Do We Prevent It?

Let us now praise human ingenuity. Millions of years ago, our ancestors first wrapped opposable thumbs around sticks and stones and turned them into tools—and weapons.

By Alan Drummer

Today, in less than a lifetime, the Internet has become the most promising and ingenious communication tool in human history. At the same time, it's also become a gateway for attacks and crimes that are getting more frequent, damaging, and inventive.

The stage is set for a whole new level of boldly conceived action—as it was in September 2001.

The systems that support billions of people around the globe—running services such as

power, water, telecommunications, banking, commerce, air traffic, and health—depend increasingly on the Internet. And the digital opportunity to do good—or evil—expands daily.

How do we minimize risks in the cyber world? Both national and global interests need protection. Where do we look for leadership in strengthening cybersecurity, and what should the priorities be? A broad collaboration is needed.

To lay out some key questions that need to be answered in cybersecurity, *CIO Digest* spoke with several key industry executives and analysts.

What's at stake?

The real threat isn't just the potential of a broad, disruptive cyber attack, many observers point out. It's the increasing incidence of silent, narrowly targeted online theft that is already underway. Most online crimes are purely for profit. Some might be for the additional purpose of helping to finance terrorist organizations.

"My fear is that if we have a catastrophic digital event governments could end up doing more damage trying to fix the problem than the act itself caused," says Rob Enderle, president and principal analyst of the Enderle Group.

Politics and the potential for big attacks aside, cybercrime puts everyone at risk. A single data breach can be large enough to ruin a company. A single act of data sabotage could undermine public confidence in a stock exchange or cause a run on a bank. "Financial thieves, if left unchecked, can do almost as much damage to our infrastructure as terrorists can," observes Enderle.

Where do we look for leadership?

In May 2009, President Barack Obama called for the appointment of a National Cybersecurity Coordinator, reporting to the National Security Council and the National Economic Council. As this article went live, the job was still not filled.

The difficulty filling it might be because the National Cybersecurity Coordinator needs to be a National Cybersecurity Czar, says Enderle. "Nobody wants the job because of the gap between responsibility and authority," he says, suggesting that the job should be similar in authority to Director of National Intelligence and report directly to the president.

Once appointed, and whatever the title, this new official will set national cybersecurity priorities.

What should the priorities be?

The first goal of the Cybersecurity Coordinator should be to protect

“My fear is that if we have a catastrophic digital event governments could end up doing more damage trying to fix the problem than the act itself caused.”

– Rob Enderle, President and Principal Analyst, Enderle Group

government assets, says Enderle. "The biggest problem with cybersecurity is that the complexity of the environment that has to be secured is unmanageable," he notes. "The first step is to turn it into something that can be managed. Then that person can apply corrective action."

That means tackling a federal security sprawl. Dozens of departments have their own rules and mandates, including the Securities and Exchange Commission, Food and Drug Administration, Federal Energy Regulatory Commission, and the department of the Treasury and Department of Homeland Security, according to the Government Accounting Office.

Adds Enderle: "Once the government is protected and on an even keel, the second step is then to move out and start aggressively protecting, to a great extent, the citizens and businesses in the country. But the government can't make other people safe if it isn't safe first."

How should the public and private sectors work together?

What the private sector needs from the federal government is assistance in setting standards, says Art Gilliland, vice president, product management, Enterprise Security Group at Symantec.

"For instance, a government organization such as the National Institute of Standards and Technology (NIST) can make certain encryption

requirements part of the Federal Information Processing Standards (FIPS)," Gilliland observes. "Industries such as financial services can then adopt FIPS-certified products and receive a promise that a given encryption technology has been vetted."

A number of observers point out that the five-year-old Federal Information Security Management Act (FISMA) needs to be updated and given teeth that enable enforcement.

Adds Gilliland: "The government should work with the private sector on developing an understanding of core cybersecurity challenges. And then private sector companies should research the problem further and develop technologies to solve it."

What can the private sector do wrong?

Other observers feel the marketplace should be left alone so it can establish its own cybersecurity standards. More than 85 percent of the Internet infrastructure is privately owned by telecommunications companies, several observers point out, and they're skeptical that government can provide better security leadership than the marketplace.

But government direction is necessary in cybersecurity, states Enderle. "If you could rely on private industry to do things in the best interest of its citizens, you wouldn't mandate things like seat belts, speed limits, and gun control laws."

“We are at a point where security is much bigger than firewalls and antivirus software and blocking a few things. Cyber security is now everything.”

— Jon Oltsik, Senior Analyst, Enterprise Strategy Group

The problem is that the private sector too often focuses on economic gains instead of problems that can seem overwhelming. Notes Enderle: “We’ve had multiple demonstrations from the dot-com collapse to the recent economic collapse that would indicate that businesses don’t make good judgments when it comes to trying to balance economic goals and security goals.”

What can the public sector do wrong—and right?

It’s also true that heavy-handed cybersecurity regulations can easily destroy businesses, Enderle concedes. “You need to have a balance,” he says. “The government needs to demonstrate how to do cybersecurity right first, and then by a combination of demonstration and law, pass that down to the private sector.”

The key requirement is that the government must first implement within itself any regulations it expects others to observe, Enderle contends. “A lot of this stuff isn’t easy, and often people in power dictate the impossible because they simply don’t realize how difficult it is.”

The government should use the carrot and not just the stick in cybersecurity, says Adam Rak, senior director of public affairs at Symantec. For example, some states penalize companies if they don’t notify consumers once their personal information has been exposed in a data breach. “But the State of California, which had the first data breach law in the United

States, has the incentive that if a company is using encryption and data is exposed, then the data is deemed not usable. It’s not defined as a breach because there are no risks to the consumer,” Rak says. “That’s a constructive incentive for good security practices.”

It’s important to have good congressional oversight of any government efforts to regulate cybersecurity, says Jon Oltsik, senior analyst at Enterprise Strategy Group. “We need a watch dog mentality from Congress to prevent cybersecurity from becoming a boondoggle,” he continues. “There is evidence to suggest that there are already some boondoggle qualities to it. I’d really like to make sure we don’t get \$500 hammers here.”

Are there successes we can learn from?

According to Rak, one good model of the kind of public/private sector teamwork needed in cybersecurity is the recent effort to develop a smart grid for delivering electricity. The smart grid is modeled after the Internet and will deliver and manage energy information nationwide to optimize alternative energy use and cost-effectiveness.

NIST has led the charge to develop smart grid standards quickly, before billions of dollars are allocated from federal stimulus funds. Security will be an important part of the new standards, Rak says, and the collaborative process of developing standards has made the administration and Congress more

prepared for what should be done next in cybersecurity.

What international cooperation is required?

The work can’t happen in the United States alone. New international outreach and agreements for enforcement and extradition are necessary for better cybersecurity, a number of observers say. “Many botmasters are based in Eastern Europe, and we can’t touch them,” Enderle observes. “Some private companies like Microsoft have been aggressive in going after and stopping people who are overseas from doing harmful things. But probably less than 10 percent of cybercrimes originating in other countries can be acted on by traditional law enforcement agencies.”

It’s big picture or no picture

The mistake in cybersecurity at any level, according to Oltsik, is to think small. “If you look at this at the tactical level of ‘I’ve got to encrypt my laptops and I’ve got to put data loss prevention in my network gateways’, then you’re not solving the problem,” he says. “That’s the ‘band-aid on the bullet hole’ mentality. We are at a point where security is much bigger than firewalls and antivirus software and blocking a few things. Cybersecurity is now everything. We live in a digital world, and so we need to have comprehensive digital security. And the sooner we realize that the better.” ■

Alan Drummer is Creative Director for Content at NAVAJO Company. His work has appeared in the Los Angeles Times, San Francisco Examiner, Create Magazine, and on The History Channel.



Commenting in This Article

- > **Rob Enderle**, President and Principal Analyst, Enderle Group
- > **Jon Oltsik**, Senior Analyst, Enterprise Strategy Group
- > **Art Gilliland**, Vice President, Product Management, Enterprise Security Group, Symantec
- > **Adam Rak**, Senior Director for Public Affairs, Symantec