THE WALL STREET JOURNAL

Everyone Should Pay for Cyber Defense

The threat to companies and critical public works is grave enough that protection is a national responsibility.

By MARTIN FELDSTEIN

The United States is vulnerable to cyberattacks by unfriendly nations and nonstate actors. Attacks through the Internet are now stealing billions of dollars of intellectual property from American businesses. Internet attacks can also bring down such critical infrastructure as the electricity supply, the air-traffic system and the stock market. Congress can and should act to protect us from this widespread and increasing danger.

The attackers use computer programs to look for openings in the computer systems of companies. They also send seemingly harmless emails to company employees which, when opened, provide entry to the company's internal networks. The attackers may be foreign governments or the foreign companies that those governments assist. Governments or terrorist groups that lack the technical capability to mount such attacks can now buy the services of skilled hackers who will do it for them.

Internet attacks on critical infrastructure can create a threat to national security even before they inflict any actual damage. A foreign enemy that gains access to the computer control systems of U.S. companies can embed malicious computer code by which the hacker can cause that system to malfunction. A foreign government that has planted such malware in the electricity system of a major U.S. city could credibly threaten to trigger it at a time when the U.S. acts to protect interests or allies abroad. That threat could block the use of our military capability.

Fortunately, the U.S. National Security Agency has the technical ability to recognize most malware coming through cyberspace from around the world. It can block suspicious messages and scan for potentially destructive malware. The NSA's technology is not foolproof but it could stop a large fraction of the dangerous Internet messages aimed at America.

That technology is currently being employed to protect the U.S. military. But those of us whose email addresses do not end with .mil are not being protected. The computers of the U.S. government (.gov), of the nation's industrial and financial institutions (.com), and of our research universities (.edu) are not protected.

There are two barriers to providing that protection. Civil-liberty advocates and others are understandably concerned about the possibility of the NSA (a part of the Defense Department) intercepting and examining emails aimed at American individuals and companies. The NSA therefore lacks the legal authority to provide the protection we need.

The second problem is the cost that companies that are part of our nation's critical infrastructure (the electric power companies, airlines, banks and others) would face if required to protect themselves from malicious attacks.

There are solutions to both of these problems that Congress should adopt as it develops legislation to deal with cybertheft and cyberterrorism. First, to protect privacy, there is no need for any person at the NSA to review the content of suspicious emails. The NSA's computers could stop the email as it enters the United States and turn it over to the Department of Homeland Security. The NSA could be legally barred from doing more than stripping off the potentially dangerous message.

The Department of Homeland Security, a completely domestic agency, could then review the content of the email or could notify the intended recipient that a potentially dangerous email had been received. The target recipient could have an agreement with the DHS choosing what happens next: authorizing the DHS to examine the content or to destroy the email or to reroute it to a safe email address where the company could examine it.

While ordinary manufacturing and service companies that are not part of the critical infrastructure should decide for themselves how much they want to spend to protect their computer systems, we all have a stake in protecting the critical infrastructure. A failure of the electric grid or the stock market computers or the railroads would hurt us all.

The infrastructure companies should be required to meet a high standard of protection and to cooperate with government agencies in preventing incoming malware. But the cost of doing that should be born by the country as a whole, just as we pay for the military or other public goods like the weather service. If necessary, funds should be diverted to cyberdefense from other areas of the military budget.

Protecting the nation from cyberattacks that steal technology and that can disrupt our daily lives should be at the top of the government's agenda.

Mr. Feldstein, chairman of the Council of Economic Advisers under President Ronald Reagan, is a professor at Harvard and a member of The Journal's board of contributors.