Guest Comment

Cybersecurity: How much is too much?

By Lawrence A. Gordon

Business and government need to respond decisively to growing concerns about hacking and cyber attacks, but we would do well to remain carefully analytic in answering the big question: Are we spending enough as a nation on cybersecurity?

The threats and vulnerabilities are very real, as has become clear with the recent disclosures by WikiLeaks of highly classified diplomatic documents from the federal government's classified computer network. This debacle notwithstanding, it's entirely possible to overreact. We need to analyze the solutions as carefully as the problem.

The battle to keep cyberspace safe is difficult to win. All one need do is follow the news to see that cyber crime is on the rise. Indeed, calls for more — even much more — spending on cybersecurity echo in the hallways of government agencies, corporations and universities. Politicians concerned about national security also call for spending more on cybersecurity. The recent disclosures by WikiLeaks certainly sent a jolt to the diplomatic community and serves to remind us of the enormity of the stakes.

Studies show that these warnings are being heeded, in that cybersecurity expenditures are growing at a rapid rate. Consequently, it is important to consider a new question: Will there ever be a point where we are spending enough on cybersecurity? My answer to this latter question is a resounding yes! Indeed, many organizations (including governments) may have already reached, or even passed, that point.

Organizations do not have infinite resources that can be devoted to cybersecurity. In fact, these expenditures compete for the same resources required for other activities within an organization, such as producing new products or services, paying higher salaries and providing employees with better health benefits.

Organizations in both the private and public sectors need to consider cybersecurity spending in a similar fashion by evaluating the costs and benefits. Applying this economic lens to cybersecurity will not only help organizations arrive at appropriate spending levels, but will force them to prioritize and consider the most efficient allocation of these resources.

Regrettably, most organizations don't do this, placing cybersecurity in a special category and arguing that normal economic principles cannot be applied. They all too often assume that it is impossible to quantify the benefits associated with cybersecurity. When it comes to national security, this "nonquantifiable benefits argument" is especially deafening — and flat-out wrong. Yes, it is difficult to quantify the benefits derived from cybersecurity initiatives, but that is not a valid excuse for failing to try. Organizations should make the best possible approximation of benefits, and then compare these to the costs associated with the same level of security. The results of that comparison should be the basis for allocating funds. Then, decision makers should keep tabs on the situation to make needed reallocations.

By following the above process, many organizations may find that the biggest problem is not how much they are spending on cybersecurity, but rather how they are allocating the resources. The key is for organizations to recognize that 100 percent security is not possible, and to make sure they're getting the "biggest bang for the buck."

Calls for more spending on cybersecurity are generally well-intentioned. However, actions to assure the security of our electronic networks need to be grounded in solid cost-benefit analysis if we are to address the right priorities. Then, and only then, will organizations be in a position to determine if they are spending too little, too much or just the right amount.

Lawrence A. Gordon is the Ernst & Young alumni professor of managerial accounting and information assurance at the University of Maryland's Smith School of Business and a faculty researcher at the UMD Cybersecurity Center.