The president has announced a new Commission on Enhancing National Cybersecurity and appointed his former national security advisor and the former CEO of IBM to lead it. Together, they have an opportunity to put the country on a path towards real cybersecurity. As they begin receiving briefings, they will soon find themselves overwhelmed with complexity and mired in technological minutiae. While there are undoubtedly aspects of the cybersecurity problem that demand complex technological solutions, we submit that the two most beneficial recommendations they can make are more straightforward. The first is to do everything possible to eliminate the vulnerabilities on which attackers depend. The second is to treat cybersecurity principally as a management problem rather than as a technology problem.

The reason you cannot read the news without learning of another hack is that attackers have an almost unlimited and constantly growing set of potential targets. Why? Think of “hacking” in the cyber context as a short-hand for exploiting vulnerabilities. The persistence of these vulnerabilities reflects the absence of incentives for developers to create secure software. In an era before software ran critical applications, this was tolerable; it is acceptable no longer. The problem is only getting worse with the growth of the Internet of Things, which connects more of our devices and our lives to the Internet but without much thought to security. In the ongoing debate about cybersecurity, there have been many sound proposals for investment in offensive and defensive cyber capabilities along with a skilled workforce able to employ these capabilities. Those are necessary moves, but they are themselves insufficient because they do not address the underlying vulnerability problem.

Improving cybersecurity for the long run requires doing everything possible to eliminate exploitable vulnerabilities. This will require a mix of carrots and sticks. The market has not yet sufficiently incentivized security. As a result, we may need to encourage industry to produce secure software by holding them liable when they don’t. Government regulates safety and security in other industries, and similar standards may at some point be necessary for software.
But when companies do acknowledge vulnerabilities in their products and make timely efforts to fix them, they should be rewarded and shielded from liability.

Some will be quick to counter that imposing liability and regulation risks stifling innovation in one of the most powerful and transformative sectors of the U.S. economy. With its mix of public and private sector commissioners and an inclusive work process, we believe President Obama’s cyber commission will be well positioned to address the liability issue in a way that breaks the cycle of cyber insecurity without unduly harming the competitiveness of our software sector.

In addition to leading the way towards the elimination of vulnerabilities, Obama’s commission should examine how organizations in both the private and public sectors treat cyber issues. Too many senior managers see cybersecurity as a technology problem and delegate responsibility for it to technical experts who are neither qualified nor empowered to make decisions on behalf of their organizations. Shifting the lens through which managers see cyber issues is imperative: today’s leaders must own cybersecurity. They need to educate themselves on the risks their organizations face, require their subordinates to monitor and reduce those risks, and then be held accountable for cybersecurity failures.

Obama’s commission has the opportunity to shape the agenda for cybersecurity for the next administration and beyond. The challenges posed by our state of near-permanent cyber insecurity are only beginning to become apparent. The commission should not be expected to solve every problem, but with a focus on reducing vulnerabilities and framing the task as a management challenge, they can chart a wise course for how to improve America’s cybersecurity.

_Roady is a doctoral student in the Department of History at Columbia University. Sulmeyer is the director of the Belfer Center’s Project on Cyber Conflict at the Harvard Kennedy School. They worked on cyber issues together for several years at the U.S. Department of Defense. The views expressed are theirs alone._