The modern Internet has wrought tremendous changes in the world; allowing individuals to connect easily across continents, business to be conducted in innovative ways, and for nearly instantaneous access to formerly unimaginable stores of information. With all of the changes, the Internet has also altered the landscape of risk – allowing for new opportunities and exposing individuals and groups to novel threats. The world has been quick to adopt the Internet and its attendant technologies but has not always considered what steps would be necessary to prevent or even mitigate these new threats. While there were previously warning signs, the past few years have highlighted the dangers individuals, and society at large, face if we continue to fail to address these threats.

The world now relies on the Internet of Things to watch over and secure their homes; hospitals and cities store their essential data digitally, either locally or in the cloud; and utilities rely on industrial control systems to maintain service over vast geographic areas. While these changes have improved the lives of many, security is too often a secondary thought – if that. Both hospitals and cities have repeatedly been the victims of ransomware attacks. Utilities, including water treatment facilities and electric grids, have been the focus of cyber-attacks. Even our homes have suffered the consequences of inadequate security. These trends are unlikely to reverse course and may intensify if COVID-19's effect on remote work lasts.

Immediate action is necessary to improve the cyber defense of the United States. To that end, this is the first article in a series which will evaluate what can be done to reduce the risks posed to American civilian computer systems by connected technologies and systems. In doing so it will consider what steps can be taken and suggest reasonable steps that can be taken by different governmental bodies as well as actions that private industry should consider taking on their own. Some changes can be implemented in a top-down approach where laws or regulations force new behaviors. Other improvements will require cultural changes such as recognizing the value of secure products even if might cost more or in improving cyber literacy. These actions will take time to have their full effect and no one action can sufficiently reduce risk; however, taken together, these actions will reduce the staggering financial and national security costs of cyber-attacks.

While the threats posed by a failure to act are very real, it is important to remember the goal of information security. It is not to remove all threats by stopping any and all risky behavior. Instead, information security should seek to minimize reductions in functionality as it maximizes risk reduction. This equation does have a real up-front cost. Put simply, it costs more to add security controls to devices, systems, and programs. It will take time and effort to better educate individuals and organizations about good cyber practices. Unfortunately, these costs are not one-time expenses either. Importantly, however, these costs do pay dividends by saving companies money, securing the well-being and personally identifiable information of individuals, and by better protecting national interests and perhaps even constitutional rights.[1] By investing in these changes early on, the United States and its constituent individuals and organizations will reduce long-term costs and mitigate unforeseeable harms.

[1] The author, Kelsey Cora Skaggs, describes the effects of government surveillance on user behavior when they know they are being observed. This same effect is possible, perhaps even likely, when unknown malicious attackers are known to infiltrate and misappropriate specific systems.