Improving the United States' civilian cyber defense posture requires action from both the public and private sector. The government can and, as earlier articles in this series argue, must take action to incentivize and require increased cybersecurity measures. However, while the government can work to secure its own systems, by its very nature the Internet is an interconnected network. These connections cross between government systems into private networks and back again. To compound this, government networks are themselves made with privately sourced components. Private entities must therefore take ownership of the risks posed to their systems and share in the responsibility to defend against these risks. By addressing vulnerabilities, these entities not only benefit their customers, they also secure their intellectual property, protect their sensitive employee data, and promote the interests of their shareholders or other stakeholders.

One proven method of reducing risk is through organizational investment in training programs. Organizations like (ISC)^2 and CompTIA provide trainings and certifications to better prepare security professionals to address threats. Companies should look to utilize these opportunities to improve their organizational knowledge by investing in their workforce. The return on investment of such investments can be hard to measure – as are most investments in revenue negative components like security – however, organizations can look to improve their returns by offering education incentive agreements. Both the organization and the individual employee can realize benefits when companies offer their employee a free or reduced cost certification in exchange for an agreement to continue working at the organization for a set period of time. Organizations interested in maximizing employee retention might also consider coupling these agreements with other incentives to reflect the employee's improved ability to accomplish their assigned tasks. The improvements realized by these programs increase organizational security knowledge which in turn helps to reduce the risks posed to American civilian computer systems by connected technologies and systems.

Private companies must also look to increase their cybersecurity workforce. Training a competent staff is essential, however, the shortage of cybersecurity professionals discussed in the fourth article of this series is also having a serious effect on the private sector. While this need is being addressed somewhat – (ISC)^2 recently noted an additional 700,000 new cybersecurity professionals in one twelve-month period – it is still woefully shy of the estimated number needed to address the talent gap. Scholarship opportunities in exchange for an agreement to work are one tool that may work in the private sector as well; however, salaries for private sector cybersecurity work is already relatively high. As such, additional pay-based incentives may have diminished returns. One alternative, hiring from non-traditional academic programs such as a liberal arts degree or even from the industry workforce the security team is protecting, might be a more effective action. In addition to expanding the applicant pool, a diversity of thought and background can be invaluable when assessing and preparing for the ever-evolving risks cybersecurity professionals face.

Reducing cybersecurity risks is not only dependent on hiring and training a competent workforce, companies must also reevaluate how they prioritize security and profit. This can be a difficult change to make, especially when so much of business is driven by the demands of the market. Improving the security of devices, software, networks, and more does cost more and it is likely, if not certain, that some of these costs will need to be passed along to consumers. In some

markets, especially those that are very price sensitive like Internet of Things devices, these additional costs present added difficulties in the market and sale of products. Still, as new laws go into effect, such as California's Consumer Privacy Act (soon to be replaced by the California Privacy Rights Act), the cost of insecurity is likely to rise. Building a reputation for security now may help provide a competitive advantage early. Moreover, as more and more of the world's market considers the effects of insecurity, stockholders, regulators, and others become increasingly likely to see the business necessity of securing consumer devices. For companies purchasing hardware, software, or services, insecure devices may be cheaper at the time of purchase, but they carry additional risk and unforeseen future costs. This has been made all the more clear with recent cyber-attacks, especially the rise in ransomware attacks and supply chain incidents. As a result, companies must evaluate the cost of insecurity against their profitability, increased liability, reputation, and other market factors.

The size and nature of business should be considered against the specific needs of each individual company. While large companies in sensitive industries will require significant investment, small companies in non-sensitive industries may have reduced needs in addition to their smaller budgets. In this way, there is not one-size-fits-all security framework for private companies, however, private industry has a responsibility to improve upon their current security posture. Failure to do so is not only likely to result in harm to their organization, it is also likely to continue contributing to unnecessary and unacceptable risks. Mitigating these risks will help protect their companies and reduce the risk posed to their networks as well as the broader connected Internet.

As this series has tried to emphasize, a variety of players can have a direct impact in reducing the risks posed to American civilian computer systems by connected technologies and systems. While the specific actions available to each group or actor differ, all share in the collective risk and conversely, stand to benefit from the positive changes made by others. In this way, much like the Internet itself, all the parties are connected to one another. Even international organizations and friendly foreign nations stand to benefit from a more secure American civilian network. The proposals highlighted in this series provide a general roadmap to achieving this improved cybersecurity posture, but it will take decisive action by the actors discussed to make it a reality.