In 2011, the United Nations declared that access to the Internet is a human right. Ten years later amid the global pandemic of 2020-21 (and counting), access to the Internet was and is a fundamental way for people to connect to each other, and a necessity for organizations to function. For individuals, the ability to support oneself through employment hinged on being able to connect to the Internet, as 88% of businesses required employees to work from home. Education and health care went virtual. The U.S. Census Bureau reported that in the spring of 2020, 93% of students participated in online education, and similarly telemedicine became a tool to implement social distancing and address hospitals overflowing with COVID patients. Concurrently, however, cyberattacks and threats skyrocketed.

2020 was the worst year on record for data and system breaches, and 2021 is predicted to top that dubious distinction. Though a lack of cyber incident reporting requirements makes any statistical evidence incomplete, in 2020 over 1,000 data breaches occurred, impacting more than 155.8 million individuals. A 2021 IBM Security study estimated the average data breach at $4.24 million, signifying a 10% increase as compared to 2020. As cyberattacks expand in frequency and severity, large business must pay an average of $825,000 to remedy a data breach, while smaller companies face potentially unrecoverable financial risks. These concerns are magnified by the fact that one third of all cyberattacks involve small businesses, yet 60% of small business entities lack the requisite resources to employ cybersecurity protection. Furthermore, the National Association of Insurance Commissioners notes that between 50% and 75% of ransomware attacks are launched against small businesses.

Increased and sophisticated cyberattacks, focused on vulnerable organizations around the world, are deflating public trust across numerous fronts including democracy and the voting process, human rights activities, critical infrastructure, and business institutions. As organizations struggle to implement fragmented, back-end security approaches that intensify risk and vulnerability, the federal and state cybersecurity regulatory landscape continues to evolve. The Federal Trade Commission (FTC) is particularly dynamic in this area, enforcing authority under § 5(a) of the FTC Act, and requiring companies to implement reasonable security measures to protect consumers. Other federal laws, like the Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPPA), and those promulgated by the Securities and Exchange Commission (SEC) are more sector-specific, or apply solely to public companies.

In addition, states have passed legislation imposing a patchwork of security measures, including the California Consumer Privacy Act, and New York’s Stop Hacks and Electronic Data Security (SHIELD) Act. Still, intensified cyberattacks were the impetus for President Joe Biden’s recent Executive Order on Improving the Nation’s Cybersecurity, and his “call to action” to improve the nation’s cybersecurity. Such Order, in conjunction with his newly proposed $9.8 billion federal cybersecurity budget, signify that the current regulatory landscape remains insufficient to meet the needs of intensified cyber-related threats.

To incent organizational behavioral changes toward more comprehensive, front-end cybersecurity investments, this article expands the current literature exploring the role that tax law
and policy can play in bolstering U.S. cybersecurity. Specifically, the liaison between tax incentives and cybersecurity is a relatively undertheorized area of law. Security infrastructures are complex and robust, yet costly. Mere awareness of the need for increased and sufficient cybersecurity protections is futile if many businesses remain financially incapable of implementing adequate security safeguards.

Recognizing that there is not a one-size-fits-all policy that can adequately address the myriad of U.S. organizational cybersecurity needs, this article delivers a cache of tax tools to be used by policymakers, to include a Federal Cybersecurity Tax Credit specifically tailored and mapped to entity type. This article also recognizes that tax law and policy alone is inadequate to address the myriad issues surrounding cybersecurity investment. Therefore, this research examines tax policy within the overall cybersecurity ecosystem, considering the unification of tax and select non-tax measures, such as information sharing and transparency, subsidized cybersecurity infrastructure, cybersecurity injury prevention loans, cybersecurity insurance coverage, and reducing ineffective regulatory burdens to provide a more holistic and useful cybersecurity framework for business and policy makers.