The 2021 Yale Cyber Leadership Forum addressed a wide range of topics, but one consistent theme was the increasing complexity and importance of cyber policy, and cyber security in particular. In many ways this is an obvious point; the frequency of consumer data breaches, fears over the security of the 2020 U.S. Presidential election, and recent cases of espionage such as the hacking of Solar Winds have made issues of cyber security impossible to ignore. But recognizing the importance of an issue and responding well to its complexities are two different things. Once one has recognized the importance of cyber security, what is the business leader, employee, or ordinary consumer supposed to do? Deep expertise is necessary to truly understand the problems that might arise and how to address them, and few of us are experts in cyber security.

What is needed is a way to outsource all cyber security decisions to experts. Or a way to provide all leaders, employees, and consumers with sufficient education so that they can make cyber security decisions well. Neither of these options is feasible—but it might be possible to successfully combine a modified version of these options; we can seek to empower experts, educate nonexperts, and develop ways for nonexperts to make better decisions without needing to develop deeper expertise. This combined strategy has the potential to improve cyber security, while recognizing the reality that a deep understanding of cyber security risks will remain confined to a few experts.

This article uses insights drawn from speakers across the Leadership Forum to outline approaches to cyber security that recognize the need for expertise—and the relative rarity of that expertise. Four approaches are discussed. Each has its own strengths and weaknesses, and so effective cyber risk management will likely require a combination of all four.

**Market Approach**

The first approach uses market incentives, specifically insurance pricing, to encourage the adoption of best practices. Companies that insure against cyber risk have a financial incentive to understand where the current risks are and where new risks are emerging. They can also monitor the firms they insure. Thus, insurers can create incentives for firms to adopt appropriate risk-mitigation strategies, by raising rates for firms that do not adopt such strategies or by refusing to insure them altogether. At the Forum session on April 1, 2021, Peter Beshar noted that cyber insurance is already driving the adoption of best practices, such as the maintenance of back-up copies of essential files and systems that enable companies to resist ransomware attacks. This practice could be extended to consumers; consumers could pay for insurance against the costs of data breaches or
ransomware attack, with insurance companies charging lower premia to those who adopt best practices like effective password management and frequent software updates.

The benefit of this approach is that it allows both businesses and consumers to outsource much of the monitoring of cyber risk. It places the financial incentive for cyber risk management in a few insurance companies, which will then have the incentive and means to develop a deep expertise. The weakness of this approach is that it is only as strong as the insurance companies that emerge; market failures could prevent these companies from effectively pricing and monitoring risk. This approach will also be ineffective at addressing idiosyncratic risks unique to a particular company.

**Simple Rules Approach**

A second approach is to develop a few simple rules for guiding behavior. For consumers, these rules could include the two best practices of effective password management and frequent software updates. For leader of organizations, developing metrics based upon the speed of detection of cyber breaches could provide a useful benchmark for evaluating the corporation’s cyber resilience, as Dmitri Alperovitch observed. This approach empowers individual actors by teaching them certain heuristics, but then leaving the response in a particular situation to their discretion. It facilitates reliance on a broad group of people, without requiring that every individual develop a deep cyber expertise.

This approach, however, will only be effective if the rules that are developed guide behavior in ways that do, in fact, reduce cyber risk. It therefore requires a robust ecosystem of academics, think tanks, and other policy researchers that propose, debate, and disseminate rules and heuristics. This approach also brings with it the danger that individuals might overestimate their expertise; the rule-follower might mistake learning a few rules with developing a deeper understanding of the issue, leading individuals to act in ways not justified by their actual knowledge.

**Reliance on and Empowerment of Expertise**

While not everyone can become an expert, expertise obviously has a significant role to play in ensuring cyber security. Both the market and simple rules approaches rely on experts—to develop accurate risk models for pricing insurance and to develop rules that effectively promote better practices. The educational system must produce enough experts to serve these, and other, cyber security roles. Experts also need to be in the right places and must be appropriately empowered. Large organizations should have a Chief Information Security Officer that can communicate technical concerns to the rest of an organization’s leadership. As Matthew Doan
argues, cyber leaders like the CISO, “must appreciate…technical capabilities and have people to handle them” and they must be given “an influential voice in business strategy, technology decisions, and enterprise risk management.”

Public Education

A final approach is broad public education. Demand for such education exists: a recent survey found that “[m]ore than 9 in 10 Americans are concerned about their security online, and 74% of consumers say they would be likely to participate in a cybersecurity education or awareness program if their bank offered it.” And there are reasons to think that broader awareness of cyber risks can improve security. As Nathaniel Gleicher noted in the Forum on March 18, 2021, Facebook’s 2020 election misinformation monitoring was successful because the government, media, and civil society were all aware of the issue. Education could be particularly effective if paired with the simple rules described above. Teaching business leaders, employees, and consumers a few rules to follow is a simple and achievable educational target.

Conclusion

Effective cyber risk management is a complex task that requires the deep expertise of some. But non-experts, as leaders of organizations, employees, and consumers also have a role to play. This article has attempted to provide a framework that will enable non-experts to effectively promote cyber security. Insurance markets, the development of simple rules, appropriate reliance on experts, and public education together can go a long way towards improving collective cyber risk management, without requiring that every individual become a cyber security expert.