Disrupting the Cyber Status Quo

DENISE E. ZHENG

MEDIA COVERAGE OF CYBER ATTACKS HAS NEVER BEEN HIGHER THAN IT IS TODAY. Government officials and business executives around the world are more aware of cyber threats than ever before and taking measures to improve security. As a result, cybersecurity is one of the fastest-growing segments of the global technology industry with approximately $1.9 billion in venture capital funding in 2014 and hundreds of new cybersecurity startups.

In the past five years, the United States alone has enacted 34 new laws and 5 executive orders to improve cybersecurity, including to strengthen standards for critical infrastructure, cyber threat information sharing, and penalties to punish and deter bad actors. U.S. defense, homeland security, and law enforcement agencies have aggressively bolstered their capacity to defend against and mitigate cyberattacks through new strategies, doctrine, and planning, and by updating technology and hiring and training thousands of new personnel.

Despite efforts to improve cybersecurity, global cyber conflict is intensifying and there is limited to no improvement in our cybersecurity posture as a nation. Companies and government agencies are engaged in an increasingly difficult struggle against persistent and agile cyber adversaries. At the nation-state level, Russia, Iran, and North Korea are using coercive cyber attacks to increase their sphere of influence, while China, Russia, and Iran have conducted reconnaissance of networks critical to the operation of the U.S. power grid and other critical infrastructure without penalty. Meanwhile, cybercrime by non-

state and substate actors has become so profitable that it has surpassed the global market for trafficking of illegal drugs.[1] There is increasing frustration over the slow pace of change, as well as concern that a truly damaging cyber attack is unavoidable if we do not change the status quo.

The slow pace of progress can be attributed to our failure to address the root causes and key enablers of cyber crime and conflict. So what are the causes and enablers? A starting point would be to look at the cybersecurity problem as three separate, but interconnected parts.

The first is the end user. These are consumers, enterprises, and government agencies that rely on commercial information technology (IT) products and services. End users are terrible at managing their own security. At the most basic level, end users do not even know how to establish strong passwords or avoid clicking on malicious links. Larger organizations struggle with basic security practices, but they also have to deal with the challenges of managing a complex IT environment, including legacy systems that are difficult if not impossible to protect.

[1] Lillian Ablon, Martin Libicki, and Andrea Golay, "Markets for Cybercrime Tools and Stolen Data," RAND Corporation, National Security Research Division, 2014, https://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf.

The second part is the global black market for cybercrime and the malicious actors, tools, and services available in this underground economy. As many have pointed out, the economics of cyber crime skew in favor of the attacker. Exploits are easily acquired and can be reused on multiple targets, and the likelihood of detection and punishment is low. The underground marketplace for hacking tools and services—as well as the gains from hacking—are growing in size and complexity. The ease of monetizing hacking services and the spoils from hacking have transformed cybercrime from ad hoc activities conducted by lone individuals, to a highly organized and coordinated global network of specialized hackers and exploit developers.

IT vendors are the third part of the problem. These companies develop, manufacture, and sell IT products, sometimes riddled with exploitable software vulnerabilities. In other business sectors, from automotive and medicine and medical devices to children's toys, there are strong precedents for product liability holding companies responsible for manufacturing and design defects and failure to warn about risks associated with using the product. In contrast, most software license agreements make companies immune to liability for damages or losses caused by software flaws. Immunity from liability in this context enables companies to get away with developing insecure products, creating fodder for the undergrown marketplace for malicious cyber activities, and it asymmetrically exposes enterprise and consumer end users to risk.

U.S. government policies and regulation have focused on securing the end user (consumers, enterprises, government agencies), primarily through information sharing, promoting the adoption of standards and best practices, and other incentives. While improving security at the end user is a critical piece of the problem, the approach is similar to promoting holistic medicine as a cure for communicable diseases. Improving the security of commercial IT products and disrupting the enablers of black market cybercrime, however, could have a game-changing effect on our cybersecurity posture.

Law and policymakers have shied away from tackling the root causes and key enablers of cyber crime and conflict.

Law and policymakers have shied away from tackling the root causes and key enablers of cyber crime and conflict. This is usually due to a lack of understanding of the issues—either because of their technical complexity or because of political pressure from businesses that fear regulation or privacy advocates who fear "Big Brother." In the absence of a major cyber attack on the United States, political, legal, and resource constraints on government action will likely persist. But action to address root causes and enablers of cyber crime and conflict need not contradict these political and business dynamics; in some cases, addressing them may not even require changes in policy or law. Much can be done by the handful of companies that provide the majority of products and services that comprise the Internet and computer-operating systems, through more focused nudging and guidance from government. □