There's No Silver Bullet for Cybersecurity

As AI, the metaverse, and quantum computing advance, cybersecurity will become an increasingly complex issue. **by Thomas P. Vartanian**

Published on HBR.org / April 26, 2023 / Reprint H07LV3

HBR Staff/Mirage C/Getty Images

Government officials in the U.S. and the UK recently took victory laps after reporting a 15% reduction in ransomware attacks. Ironically, as both governments issued press releases and touted their accomplishments, a global ransomware blitz by a presumed group of Russian and Chinese hackers was underway. The attacks infected an estimated 5,000 victims in Europe and the U.S. with ransomware, demonstrating the two-steps-forward, one-step-back nature of fighting the war on cyber terror.

Some years ago, the CEO of a major financial institution called me after his company had suffered an online attack. By the time I appeared in his office, customer data was likely already circulating on the dark web. As the company’s counsel, I needed to determine not only what happened, but what — and when — we could tell regulators and customers. Access to the company’s servers was thought to have been penetrated through an outside service provider. When we interviewed that provider, we learned that it had obtained the hardware and software from yet other third parties who relied on still other parties (some in foreign countries), many of whom evidenced a modest sense of responsibility at best for what had occurred.

At that moment, I began to appreciate the fallibilities of an internet that had not been built to secure all the data and value on the planet. That is also when I realized how difficult it is to assign responsibility for hacks, particularly given the number of parties in the chain and the mistakes humans inevitably make in the process.

As the frequency of major breaches involving well-chronicled ransomware and cyberattacks on a pantheon of government agencies and corporations continues unabated, it raises a key question for business executives — how do you confront a virtual future that may contain more threats than profits?

The threats are numerous. In the U.S., computers in one of every three homes have been infected with malicious software, and the personal information of 47% of American adults has been exposed to cyber criminals. Perhaps no statistic speaks louder than the government’s conclusion that 600,000 Facebook accounts are hacked every day in the U.S. We should expect these numbers to continue and even increase. So, who is going to pay for this?

The Biden administration's National Cybersecurity Strategy, released on March 2, 2023, tries to answer that question. In part, it proposes that the way to overcome the structural deficiencies of the internet is to "run faster": essentially, to get ahead of cyber criminals and impose more government involvement in cyber-regulation. That has not and will not work. This proposes imposing stricter liability penalties for breaches on the private sector to alter the economic incentives that reward being first, and hardly penalize those who chase profits and ignore security standards. Even if that liability is initially imposed on software vendors, it will undoubtedly trickle down to intermediate and end-user businesses. Of that, we can be sure.

Dealing with this new world of cyber threats will become even more complex as the next big digital advancements unfold. For example, 100 million users downloaded ChatGPT in just two months to write essays, do research, and tickle their curiosity — without understanding the risks involved. 5G technologies will bridge ubiquitous human-to-human, machine-to-machine, and human-to-machine connectivity that will enable a seamless Internet of Things (IoT). That IoT will connect people, pets, household appliances, and industrial tools, making them more capable of operating, communicating, recording, monitoring, adjusting, and interacting with minimal human intervention. The business efficiencies of these new tools will be enormous, but so will the risks. Connecting products, people, wearable transmitters, and machines will create new, larger databases that can be stored, analyzed, used, and abused. Everything that is connected can be hacked, and everything will be connected.

And then there is quantum computing, which threatens to make the current technology we use to protect data and money obsolete. Computer scientists estimate that the RSA 2,048 bit encryption that most currently use to protect data could take today's supercomputers

300 trillion years to break. In comparison, 4,099 qubit computers of the near future will be able to break the same code in 10 seconds. Experts in the field expect to develop a quantum computer with 1,000 qubits in the next few years, pushing us further down the path to either better protecting or further dismantling every digital security system that exists today. Whether quantum computing is ultimately a threat or a marked enhancement of the human condition turns on who gets there first and what they do with it. Not incidentally, China plans to get there first, and is rapidly outspending and outpacing the U.S. in efforts to do so.

Finally, there is the metaverse — the next generation of the internet that will increase the stakes and the difficulty of securing the online environment by further blurring the lines between human and machine consciousness.

Governments are incapable of fixing the insecurity of the internet by themselves, and businesses are unlikely to do it until the economic pain of ignoring the insecurity becomes greater than the profits it can earn from it. There are no silver bullets beyond restructuring the internet to rely more on new secure private networks, particularly for the operation of critical infrastructure. That will require businesses, governments, and users in democratic nations to act together to transform the internet into networks that rely on the authentication of people rather than IP addresses, mandate strict rules of online behavior, and maintain cyber police (human or machine) to enforce them.

This will not be an easy or popular task, but the alternative of cyber chaos and the potential disappearance of electricity, money, and health services is clearly unacceptable. A new internet will also require a new form of oversight, rather than the cops-and-robbers style that we have had. This new wave of regulation will demand a more decentralized, collegial form of oversight where the private and public sectors work together to share data and build policy consensus. This will all take time and strong leaders to get it done. We don't seem to have much of either at the moment.

This article was originally published online on April 26, 2023.

TV

Thomas P. Vartanian is the author of *The Unhackable Internet: How Rebuilding Cyberspace Can Create Real Security and Prevent Financial Collapse*. He is a former federal bank regulator, counselor, and academic, and is currently the Executive Director of the Financial Technology & Cybersecurity Center.