Bruce Schneier
Harvard University

What Will It Take?

What will it take for policy makers to take cybersecurity seriously? Not minimal-change seriously. Not here-and-there seriously. But really seriously. What will it take for policy makers to take cybersecurity seriously enough to enact substantive legislative changes that would address the problems? It's not enough for the average person to be afraid of cyberattacks. They need to know that there are engineering fixes—and that's something we can provide.

For decades, I have been waiting for the "big enough" incident that would finally do it. In 2015, Chinese military hackers hacked the Office of Personal Management and made off with the highly personal information of about 22 million Americans who had security clearances. In 2016, the Mirai botnet leveraged millions of Internet-of-Things devices with default admin passwords to launch a denial-of-service attack that disabled major Internet platforms and services in both North America and Europe. In 2017, hackers—years later we learned that it was the Chinese military—hacked the credit bureau Equifax and stole the personal information of 147 million Americans. In recent years, ransomware attacks have knocked hospitals offline, and many articles have been written about Russia inside the U.S. power grid. And last year, the Russian SVR hacked thousands of sensitive networks inside civilian critical infrastructure worldwide in what we're now calling Sunburst (and used to call SolarWinds).

Those are all major incidents to security people, but think about them from the perspective of the average person. Even the most spectacular failures don't affect 99.9% of the country. Why should anyone care if the Chinese have his or her credit records? Or if the Russians are stealing data from some government network? Few of us have been directly affected by ransomware, and a temporary Internet outage is just temporary.

Cybersecurity has never been a campaign issue. It isn't a topic that shows up in political debates. (There was one question in a 2016 Clinton–Trump debate, but the response was predictably unsubstantive.) This just isn't an issue that most people prioritize, or even have an opinion on.

So, what will it take? Many of my colleagues believe that it will have to be something with extreme emotional intensity—sensational, vivid, salient—that results in large-scale loss of life or property damage. A successful attack that actually poisons a water supply, as someone tried to do in January by raising the levels of lye at a Florida water-treatment plant. (That one was caught early.) Or an attack that disables Internet-connected cars at speed, something that was demonstrated by researchers in 2014. Or an attack on the power grid, similar to what Russia did to the Ukraine in 2015 and 2016. Will it take gas tanks exploding and planes falling out of the sky for the average person to read about the casualties and think "that could have been me"?

Here's the real problem. For the average nonexpert—and in this category I include every lawmaker—to push for change, they not only need to believe that the present situation is intolerable, they also need to believe that an alternative is possible. Real legislative change requires a belief that the never-ending stream of hacks and attacks is not inevitable, that we can do better. And that will require creating working examples of secure, dependable, resilient systems.

Providing alternatives is how engineers help facilitate social change. We could never have eliminated sales of tungsten-filament household lightbulbs if fluorescent and LED replacements hadn't become available. Reducing the use of fossil fuel for electricity generation requires working wind turbines and cost-effective solar cells.

We need to demonstrate that it's possible to build systems that can defend themselves against hackers, criminals, and national intelligence agencies; secure Internet-of-Things systems; and systems that can reestablish security after a breach. We need to prove that hacks aren't inevitable, and that our vulnerability is a choice.

Digital Object Identifier 10.1109/MSEC.2021.3063800
Date of current version: 14 May 2021

continued on p. 63

 Copublished by the IEEE Computer and Reliability Societies 1540-7993/21©2021IEEE

 continued from p. 64

Only then can someone decide to choose differently. When people die in a cyberattack and everyone asks "What can be done?" we need to have something to tell them.

We don't yet have the technology to build a truly safe, secure, and resilient Internet and the computers that connect to it. Yes, we have lots of security technologies. We have older secure systems—anyone still remember Apollo's DomainOS and MULTICS?—that lost out in a market that didn't reward security. We have newer research ideas and products that aren't successful because the market still doesn't reward security. We have even newer research ideas that won't be deployed, again, because the market still prefers convenience over security.

What I am proposing is something more holistic, an engineering research task on a par with the Internet itself. The Internet was designed and built to answer this question: Can we build a reliable network out of unreliable parts in an unreliable world? It turned out the answer was yes, and the Internet was the result. I am asking a similar research question: Can we build a secure network out of insecure parts in an insecure world? The answer isn't obviously yes, but it isn't obviously no, either.

While any successful demonstration will include many of the security technologies we know and wish would see wider use, it's much more than that. Creating a secure Internet ecosystem goes beyond old-school engineering to encompass the social sciences. It will include significant economic, institutional, and psychological considerations that just weren't present in the first few decades of Internet research.

Cybersecurity isn't going to get better until the economic incentives change, and that's not going to change until the political incentives change. The political incentives won't change until there is political liability that comes from voter demands. Those demands aren't going to be solely the results of insecurity. They will also be the result of believing that there's a better alternative. It is our task to research, design, build, test, and field that better alternative—even though the market couldn't care less right now. ■

Bruce Schneier is a security technologist, fellow, and lecturer at the Harvard Kennedy School, Cambridge, Massachusetts, USA, and the chief of security architecture of Inrupt, Inc. He blogs at www.schneier.com. Contact him at schneier@schneier.com.

Digital Object Identifier 10.1109/MSEC.2021.3074226