Equifax and Our Broken Computer Industry

Oct. 2, 2017 The world has come to depend on systems designed to fail.

Originally produced on Sept. 25, 2017 for Mauldin Economics, LLC

By George Friedman

The Equifax hack ought to have been the last straw in the saga of our inept computer industry. Critical information on the vast majority of American families was compromised. To say that this was not a rare phenomenon understates it. There has been an endless array of stolen information, from the recent theft of still proprietary stock information from the Commerce Department to the theft of emails from the Democratic National Committee.

The probability that information committed to computers will remain confidential has become slim at best. It must be assumed that if people wish to steal information, they will.

The "Stupid User" Defense

The computer industry has developed a defense that most industries have tried at one point or another: the "stupid user" defense. When a hack occurs, the spotlight turns to the victim, who is said to be responsible for preventing such attacks. Consider my favorite attack: phishing. A phishing attack happens when someone receives an email and clicks on a malicious link contained in the email. This triggers a process where the program linked to the email searches for, finds, and transmits information from the computer to the sender of the email.

The view of the computer industry is that the responsibility for this attack rests with the stupid user who clicked on the link. The computer industry has made it clear that you should never click on a link from an unknown sender. Announcing this has discharged the industry's responsibility. But assume that a company had 5,000 employees. The probability that one person out of 5,000 would not click on the link is near zero. An effectiveness rate of 99.98% in preventing clicks would not be enough to prevent potential disaster. A business or individual would have to prevent all mistakes perfectly and permanently.

At a higher level, the industry blames the stupid administrator. The security sold with servers, laptops, and the rest is primitive. In selling the equipment, the rule is caveat emptor, let the buyer beware. It is the job of the IT administrator not only to keep things running but also to acquire and maintain a host of security hardware and software to keep the system secure. The problem is not that these tools are fiendishly expensive but that they constantly become obsolete and have to be reconfigured or replaced.

Attackers' Advantages

There is a cadre of criminals and vandals that is constantly trying to circumvent security systems. The advantage is with the attacker. The defender must reconfigure his system to meet a new attack, which the attacker will make certain is novel and therefore not anticipated. This new attack must be detected by users and communicated among them, then a defense must be developed and implemented. This process takes days or weeks.

For midsized and small businesses, maintaining constant awareness of new attacks and having the expertise to block them is absurd. And for the very largest businesses, the resources are never enough to prevent all errors in protection. If the attacker fails, no one knows about it and he will live to fight another day. If the defender fails—and the computing system is so shabbily built that it generates failures by its own lack of sophistication—he is all over the front pages.

We all know that computing systems are liable to attack. We also know that the system is designed for failure. At some point, someone will commit an error and click on a malicious link. Given the increasing tempo of attacks, expecting that administrators will never fall behind the curve is ridiculous. We also know that computer companies have pushed the responsibility for security on users, telling them to acquire third-party software and hardware. Security not only costs significant amounts of money, but it also requires expertise in acquiring, integrating, and configuring the equipment. Finally, the third parties are themselves liable to error.

The problem, as I have written before, has to do with the primitive nature of computers. The basic structure of hardware and software was created to allow upgrades and third-party software to run on the systems. Since much of this came from outside vendors, authenticating the legitimacy of the code was difficult. It still is difficult. Computers can play vastly complex games, but they cannot identify malicious code. Computer companies solve the lack of evolution in computer security by pointing at the users. Try this in any other industry and I am reasonably certain that the lawsuits would be flying, regardless of what the fine print on contracts said.

But it is not just the legal issue—although I am fascinated that no one that I know of has brought suits against the computer industry for knowingly selling defective products. Rather, my concern is geopolitical. The world has become utterly dependent on computing. I am typing this on a computer, and my personal information was compromised on a computer. The attacks are mounting, and the vulnerability of our financial and military systems—and those of the rest of

the world—are not only vulnerable but under constant attack. We cannot abandon computing, nor can we risk the consequences of using these systems. Nor will the “stupid user” explanation work when most users are as ignorant of computing as they are of the internal combustion engine.

The computer and the car have become utilities where the manufacturers are given great value by society. Cars have roads, and computers have access to the Internet. Both have utilitarian necessity. But cars are expected to maintain certain safety features. It would seem reasonable that an industry whose failures can wreak havoc globally should be expected to build security into its own systems.