FOREIGN POLICY RESEARCH INSTITUTE
E-NOTES
"A nation must think before it acts." - Robert Strausz-Hupé

MAY 2014

CYBERSECURITY: A NATIONAL SECURITY CRISIS IN MICROCOSM

By Lawrence Husick

Lawrence Husick is an FPRI Senior Fellow, Co-Chair of FPRI's Center for the Study of Terrorism, and Co-director of FPRI's Wachman Center project on Teaching about Innovation.

With its recommendation on April 28, 2014 that one of the most popular Internet browsers, Microsoft's Internet Explorer, not be used because of a flaw that could allow unlimited access to a personal computer running the Windows operating system (http://www.kb.cert.org/vuls/id/222929), US CERT, the United States Computer Readiness Team of the Department of Homeland Security surprised even the most jaded cyber-observer. This announcement, like the thousands that have preceded it (http://www.us-cert.gov/ncas/alerts/), hinted at a little-appreciated fact of modern life: the Internet, and the hardware and software on which it depends, is both the most complex technological system ever constructed, and the most vulnerable. Network infrastructure designed to be transparent and efficient is now assaulted using techniques of such complexity that even one misplaced line or punctuation mark buried in millions of lines of code may bring about a serious breach. Open source and proprietary system alike are targets, and regardless of the resources available, organizations from Apple to volunteer code maintainers working on obscure functions can make simple errors of potentially great consequence. Even the US nuclear weapons arsenal is not invulnerable, as noted in a January 2013 report from the Defense Science Board (http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf).

Those taking advantage of the state of the Internet and of computing in general now range from "script kiddies" – teens intent on exploiting and exploring the hidden world just beyond any Internet portal, to cybercriminals, stealing credit card and identity information, to cyberterrorists who disrupt and deface to score political points, and cyberwarriors, including the United States' own NSA, Cybercommand, and FBI. Despite the recent warning from US CERT, it is not even clear that all parts of the United States government are on the same cybersecurity page. Recent press reports have stated that the National Security Agency knew about and exploited the "HeartBleed" flaw for many months, without warning either other government agencies or the public about the danger. The message, clear to all by now, is that no electronic system is entirely secure, and that it is now up to individuals to protect their systems and information from all who would compromise and exploit it. The issue for most, however, is one of skill and knowledge: how, without a computer engineering degree and years spent at a keyboard, can we improve security and safeguard our information?

On the systems level, organizations and activists are working to secure the Internet and computer systems against attack. New software is being developed to give added levels of security and encryption. Computers such as Google Chromebooks operate only on the Internet, allowing users to cede most responsibility for security, beyond the choice of a good password, to Google and its army of programmers. Other systems, such as Apple's OS X, and iOS have been developed with security in mind from the beginning, unlike older systems which had to be patched and retrofitted, never entirely successfully, with antivirus and firewall software. The issue, however, is that while newer computers are demonstrably safer to use, millions of older computers, switches, routers, modems, printers, and

other devices remain in use, and vulnerable. Our information passes through these system components, even when we upgrade to newer, better computers. There is no practical way to legislate or regulate the upgrading of all of these systems, and corporations, governments, and individuals seldom have unlimited budgets for new systems and software, together with the millions of hours required to install and implement them.

There are, however, a few rays of hope in this otherwise bleak scene. Public-spirited and entrepreneurial programmers have launched tools that allow individuals to determine whether they have been "hacked" in recent attacks on commercial and government websites. Among these tools are haveibeenpwned.com (pwned is "hackerspeak" for having your system or password breached), PwnedList and Shouldichangemypassword.com. These sites are free for individual use, and because each uses a slightly different data set, it is wise to check on all three, and follow any advice they offer, should you find that you have been "pwned".

In addition, there are good tools for choosing, using, and remembering cryptographically strong passwords, which, while not perfect, are still the first line of defense on the Internet. Yes, we know that the recommendations for long and confusing passwords, different for every site and account and changed often are impossible to follow, even for those who work at the NSA. Software tools, however, make this process relatively painless. One example of such a system is Apple's "iCloud Keychain" which comes standard on every Macintosh running OS X Mavericks, and on every iPhone and iPad running iOS7. When accessing a site that asks for a password, the Apple software offers to create a strong one, such as, for example, "LyF-G4x-vTh-NnD" and then saves it in encrypted form in Apple's cloud infrastructure, making it available again whenever you enter that website, regardless of which device (laptop, iPhone or iPad) you are using. It even works on non-Apple devices, provided that you use Apple's Safari browser. Other software products, such as 1Password and DashLane perform similar functions.

It should be clear by now that the Internet is never going to be perfectly secure. There are just too many moving parts and the complexity is beyond the comprehension of any team of experts. Security firm Kaspersky Lab has even developed a terrifying real-time map of cyberthreats worldwide (http://cybermap.kaspersky.com/). As individuals, agencies and companies, however, we can and must take more responsibility for the security of our information, if only to thwart the criminals and terrorists who would otherwise prey upon us. As in all security, our goals should be efficiency and effectiveness - not perfection. And, as Scott McNealy, the founder of Sun Microsystem famously warned in 1999, "It's the Internet. You have zero privacy anyway. Get over it."