BerkeleyLaw
UNIVERSITY OF CALIFORNIA
Berkeley Center for Law, Business and the Economy

University of California, Berkeley
School of Law
2850 Telegraph Ave, Suite 500
Berkeley, CA 94705-7220

Ph: 510.642.0532 – Fax: 510.643.7095
E-mail: BCLBE@law.berkeley.edu
http://www.law.berkeley.edu/bclbe.htm

Can Artificial Intelligence Protect Us From Cybercrime?

By Erika Kiran Solanki, .D. Candidate 2017 | November 24, 2015According to Symantec's Norton Report, the global cost of cybercrime was $113 billion in 2013. That is an astounding number. Human beings tend to be the biggest barriers to computer security in the sense that passwords are predictable, random USB drives do not cause pause, and we routinely visit less than secure websites.

The U.S. Department of Defense experiences 41 million scans, probes, and attacks a month. The U.S. military, once a vulnerable IT behemoth, is now reformed as an adept defender of its well-secured networks. According to the Pentagon, while technical upgrades and advanced technology are important, minimizing human error is even more critical. Despite the unified architecture and state-of-the-art technology, in almost every successful attack on the .mil network, people have been the weak link. Hackers capitalize on mistakes by network administrators and users, which create loopholes for successful penetration. Experts contend that simply consistent monitoring of systems—fixing known vulnerabilities and double-checking security configurations—can prevent the majority of attacks. It seems that technology can create a false sense of security. People matter as much as, if not more than, technology in building an ethos and culture that minimize risk.

The question now is whether we can set up our computers to defend our computers. Is artificial intelligence smart enough to end cybercrime? Can we build a computer that is fast enough and smart enough to defend us from hackers all on its own? According to experts, probably not. Experts contend information security utilizes weak artificial intelligence technology. Weak AI is non-sentient, user friendly, and performs superior to human ability in one or two respects. Consider Google and its super fast search engine. Google is not as smart as a human, but it recognizes human language, and it is far better at scouring the Internet for search results than a human.

A common piece of security software is the SIEM tool. The SIEM tool protects technology to the extent that it is told to block a certain type of malware and then only detects and prevents the penetration of that exact malware. Hackers can change as little as a single line of code in the malware and thus cause that threatening program to become undetectable by the SIEM tool. Human intelligence is required to identify intrusion attempts, update firewalls and SIEM tools, and monitor overall systems. It is unlikely this process will ever become fully automated.

Even if a computer is developed that can identify 100% of malicious web traffic, in all likelihood that system will not be able to prevent successful breaches. For example, there is the case of the air-gapped computer. This computer is never connected to the Internet, thus by definition, it is more secure than any firewalled device. Yet a team of researchers were able to successfully hack this computer in multiple ways, including by using heat waves, ultrasound and a low-end mobile phone.

The apparent issue is that it seems there is no "unhackable" device. Thus, artificial intelligence probably can't protect us from cybercrime. This is certainly not a job for weak AI, and while some experts contend that this is where strong AI comes in, right now, strong AI is almost in the realm of science fiction, as it is supposed to compete with human levels of intelligence and problem solving. It seems the Pentagon is ahead of the curve in its focus on building a culture

BerkeleyLaw
UNIVERSITY OF CALIFORNIA
Berkeley Center for Law,
Business and the Economy

University of California, Berkeley
School of Law
2850 Telegraph Ave, Suite 500
Berkeley, CA 94705-7220

Ph: 510.642.0532 – Fax: 510.643.7095
E-mail: BCLBE@law.berkeley.edu
http://www.law.berkeley.edu/bclbe.htm

that prioritizes user protocols and minimizes risk, and we as humans must ourselves break the pattern of being the weak link in cybercrime assaults.