Privacy, Confidentiality, and Security of Health Care Information: Lessons from the Recent WannaCry Cyberattack

Tobias A. Mattei

On 13 May, 2017 hackers started to spread a ransomware (a program that locks down all files in the infected system) to computers around the globe. According to the Europol, more than 200,000 computers in 150 countries have been victims of the cyberattack, which involved the request of a $300 ransom in order to return control of the encrypted files (Figure 1). The WannaCry ransomware took advantage of an inherent vulnerability of Microsoft Windows, which had already been previously explored by the U.S. National Security Agency (NSA) for secret surveillance purposes. Besides affecting individual computers, the WannaCry also significantly disrupted the routine operation of several large commercial and governmental institutions including Fedex, Deutsche Bahn, Megafon, Telefónica, the Russian Central Bank, Russian Railways and Russia's Interior Ministry. In the United Kingdom the cyberattack crippled the information technology systems of hospitals across the National Health Service, with the end result of operations being cancelled, hospitals being placed on diversion status, and health information documents such as patient records being made unavailable in both England and Scotland. Preliminary evidence points toward North Korea's army of hackers (which, according to recent estimates, have earned more than $1.5 billion last year from illegal cyber activities[1]) as the main culprit of what has been considered by the cybersecurity company F-Secure "the biggest ransomware outbreak in history." The frequency of this type of ransomware cyberattacks has been exponentially increasing, with several similar events reported in the United States in the past few years, the most notable one on February 2016, when the Hollywood Presbyterian Medical Center in Los Angeles ended up paying a $17,000 ransom in bitcoins to regain control of its information technology network.[2]

According to cybersecurity experts, whenever a software company such as Microsoft issues a security patch on its operational system, there is public exposure of a specific vulnerability of their software, which in turn can be easily explored by hackers for criminal activities. In this specific case, Microsoft issued a patch in March 2017 that would have protected computers from the WannaCry malware. Although the patch was free to users running recent versions of Windows, consumers with computers running older software versions (such as Windows XP) have to pay substantial amounts (up to $1000 a year per device) for the additional protection. This type of scenario raises serious ethical concerns regarding such policies from large software companies, which involve charging hefty fees for providing additional protection to software products that, although sold as having an acceptable degree of security, were ultimately found to be defective. The same degree of concern arises when public officials decide, purely on the basis of economic considerations, to avoid such additional cybersecurity costs. In this specific instance, it was publicly known that in 2015 the U.K. Secretary of State for Health Jeremy Hunt decided to stop paying Microsoft for extended Windows XP support (a deal that would have cost £5.5 million), ultimately rendering the health care information systems of the whole nation vulnerable to this type of cyberattack.

Questions about the precise definition of negligence and the required conditions for allocation of liability to those who fail to use the necessary means for preventing potential threats or accidents have been for centuries in the center of academic debates on American tort law. As a theoretical legacy of the so-called "economic analysis of law" movement from the Chicago school of economics, which has dominated this discussion during most of the 20th century,[3] in the United States there is a strong tendency toward considering such questions in terms of the cost-effectiveness of prevention.[4] A widely used legal tool for determining whether a legal duty of reasonable care has been breached was proposed by judge Learned Hand from the U.S. Court of Appeals for the Second Circuit in 1947.[5] The so-called Hand's formula states that someone's duty to provide adequate preventive measures against a possible harm is basically a function of 3 variables: 1) the probability that the accident/harmful event will occur (algebraically: P); 2) the gravity of the resulting injury if it occurs (L); and 3) the associated burden or economic costs of the precautionary measures (B). According to this formal rule for negligence calculus, a duty of due care for the defendant exists if $PL > B$.

Apart from possible theoretical criticisms of the inherent presumption of the "law and economics" movement about the supremacy of economic efficiency as the ultimate goal of law and public policies,[6] the application of this type of cost-utility approach for risk analysis in the scenario of health care information security involves deeper conceptual problems. The first one is a lack of validated tools for proper evaluation of the real damages secondary to a security breach of health care information. Can they really be simply reduced to their secondary effects in terms of appointments cancellations, delay in care, and hospital divergence of emergencies, all of which seem to constitute only the more superficial and immediately visible consequences of a greater problem? A second concern is that Hand's formula may be simply inadequate to evaluate complex scenarios such as those involving health care information security, in which there is not only risk (a situation in which the probability distribution of a certain undesired outcome can be clearly estimated) but also an essential degree of uncertainty (i.e., the absence of precise means to properly estimate or predict the associated risks).[7]

Figure 1. Screenshot of the ransom note left on the systems infected by the WannaCry worm. (Image reprinted from Wikipedia https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#/media/File:Wana_Decrypt0r_screenshot.png. This image is ineligible for copyright protection in the country of origin, in accordance to Ex turpi causa non oritur actio legal doctrine.)

Hospitals and health care facilities (in addition to 15 other economic sectors) are currently deemed by the U.S. Department of Homeland Security as part of the critical infrastructure essential to national security.[8] However, in this new era of a dynamic, global, and data-driven socioeconomic environment, it is possible that the greatest threat to the health care of civilians may come not from physical terrorist attacks to health care facilities, but rather from unexpected cyberattacks targeting the security of health care information systems.[9] Following the recent virtual calamity that crippled the whole national health care system in the United Kingdom (albeit for a short period of time), the world has learned the painful lesson that privacy, confidentiality, and security of health care information should be not only an ethical theme in the educational curriculum of health care professionals but also a first-level national security priority.

REFERENCES

1. Nikkei Asian Review. North Korea capable of hacking with WannaCry ransomware. Available at: http://asia.nikkei.com/Politics-Economy/International-Relations/North-Korea-capable-of-hacking-with-WannaCry-ransomware. Accessed May 18, 2017.
2. New York Times. Los Angeles hospital pays $17,000 after attack. Available at: https://www.nytimes.com/2016/02/19/business/los-angeles-hospital-pays-hackers-17000-after-attack.html. Accessed May 18, 2017.
3. Posner R. *The Economics of Justice*. Cambridge, England: Harvard University Press; 1983.
4. Calabresi G. *The Cost of Accidents: A Legal and Economic Analysis*. New Haven, CT: Yale University Press; 1970.
5. U.S. v. Carroll Towing, 159 F.2d 169 (2d Cir. 1947). Available at: http://law.justia.com/cases/federal/appellate-courts/F2/159/169/1565896/. Accessed May 18, 2017.

6. Hardin R. The morality of law and economics. *Law and Philosophy*. 1992;11:331-384.

7. Han PK, Klein WM, Arora NK. Varieties of uncertainty in health care: a conceptual taxonomy. *Med Decis Making*. 2011;31:828-838.

8. DHS. Critical infrastructure sectors. Available at: https://www.dhs.gov/critical-infrastructure-sectors. Accessed May 18, 2017.

9. PHE. Preparedness planning. Available at: https://www.phe.gov/preparedness/planning/CyberTF/Pages/default.aspx. Accessed May 18, 2017.

Neurosurgery & Spine Specialists, Eastern Maine Medical Center, Bangor, Maine, USA

1878-8750/$ - see front matter
http://dx.doi.org/10.1016/j.wneu.2017.06.104