The NEW ENGLAND JOURNAL of MEDICINE

Perspective

Threats to Information Security — Public Health Implications

William J. Gordon, M.D., Adam Fairhall, A.L.M., and Adam Landman, M.D., M.I.S., M.H.S.

In health care, information security has classically been regarded as an administrative nuisance, a regulatory hurdle, or a simple privacy matter. But the recent "WannaCry" and "Petya" ransomware attacks have wreaked havoc by disabling organizations worldwide, including parts of England's National Health Service (NHS) and the Heritage Valley Health System in Pennsylvania. These events are just two examples of a wave of cyberattacks forcing a new conversation about health care information security. With the delivery of health care increasingly dependent on information systems, disruptions to these systems result in disruptions in clinical care that can harm patients. Health care information security has emerged as a public health challenge.

Threats to information security plague many industries, but the threats against health care information systems in particular are growing. Data breaches, generally described as an impermissible use or disclosure of protected health information, are particularly prevalent. Nearly 90% of health care organizations surveyed by the Ponemon Institute (which does independent research on privacy, data protection, and information security policy) suffered a data breach in the past 2 years; meanwhile, 64% of organizations reported a successful attack targeting medical files in 2016 — a 9% increase in just 1 year.[1] Multiple causative factors are involved in the uptick in attacks against health care systems, but some reasons cited in that study include low organizational vigilance, inadequate staffing and funding for information technology security, insufficient technology investment, and the underlying value of health care data as compared with data from other industries.

Attackers use a variety of techniques against health care organizations. Denial of service (DoS) attacks, aimed at disrupting and disabling systems by overwhelming them with large volumes of network traffic, have targeted health care facilities.[2] Such attacks can render clinical systems unusable, with negative effects on core hospital operations, such as delays in surgical procedures, lab-result reporting, and bed management. More recently, attacks against health care organizations have taken the form of ransomware. In these attacks, an information system — for example, a database containing patient information — is encrypted in such a way that only the attacker has the "key" to unlock the data. Hospitals are faced with poor options: pay the attacker, usually anonymously in online cryptocurrencies such as Bitcoin, or rely on older backups that may not contain the most recent clinical information; even an organization that backs up every system daily could lose critical data if forced to restore from a backup. The May 2017 WannaCry attack that affected the NHS is an example. Other recent examples include an attack on the Hollywood (California) Presbyterian Medical Center that resulted in the payment of $17,000 to hackers and one on MedStar Health, which caused a temporary but large-scale computer shutdown in its network of hospitals. Payment doesn't guarantee access to encrypted data — though the ransom price could be worth the risk depending on the severity of potential data loss. More than 50% of hospitals have reported at least one ransomware attack in the past year.[3]

Although DoS and ransomware attacks disrupt systems and can significantly impair the ability to deliver efficient care, they do not necessarily expose patient information. More worrisome are attacks that result in breaches of protected health information and personally identifiable information. Such information is valuable to attackers for two main reasons. First, it has direct monetary value: attackers can sell these data in anonymous online forums that are part of what's sometimes referred to as "the dark web." For example, in June 2016, a hacker posted on the "Real Deal" dark-web marketplace offering for sale more than 600,000 medical records from three different systems, one of which was an entire electronic health record, including screen shots.[4] Medical records can be used for various fraudulent activities, including falsified claims, medical device purchasing (and reselling), and credit card identity theft.

Second, protected health information is durable. Whereas credit card numbers, insurance identifiers, and even Social Security numbers can be changed, a piece of medical history is indelible and can be used as identifying information even years after an initial breach. The data can also be used for highly targeted e-mail "phishing" campaigns to collect credentials that, in turn, give attackers access to systems and information.

The potential for manipulation of clinical systems and clinical data constitutes an additional threat. The effect of such threats on medical devices has been well described. In 2015, the Food and Drug Administration (FDA) and the U.S. Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) issued an alert regarding an infusion system that could allow an attacker to remotely control the device and alter therapy administration.[5] In January 2017, the FDA issued a similar warning for St. Jude Medical's radio-frequency–enabled implantable cardiac devices and transmitters. Fortunately, a software patch could be applied automatically to the affected transmitters.

Manipulation of patient data could be even more damaging. An attacker with access to a laboratory system could modify data — changing potassium values, for example. Unsuspecting health care providers could react to the falsified potassium values, providing treatment that could harm the patient. Radiology protocols, diagnostic reports, genetic data, progress notes, and electronic prescriptions — the list of possible targets goes on. Protecting our information systems and our health data is critical to ensuring the safe delivery of health care.

Unfortunately, protection against the myriad threats to health care data is complex, and there is no silver bullet. There are, however, ways to reduce risk. First, modern, best-practice security practices can be followed. These include data encryption, antivirus software, software updates, and two-factor authentication. Frequent backups, with robust failover mechanisms to switch to those backups, can lessen the impact of ransomware attacks. Access to protected health information and personally identifiable information can be limited to persons who absolutely require it, in keeping with "need to know" policies. Risk analyses, as required by the Health Insurance Portability and Accountability Act (HIPAA), should be performed routinely, and mitigations implemented as needed. Medical device manufacturers should follow the FDA's guidance on cybersecurity for devices. Although security processes can seem inconvenient, they are necessary to protect medical practitioners and patients.

Second, we can be both practical and intelligent about the use of technology. Systems can be designed with workflow in mind. A highly secure system that is not usable (and therefore not used) is less secure than a moderately secure system that is adopted widely. One example is password security: although password strength is important in preventing attackers from guessing passwords, it is not clear that the common practice of requiring regular password changing makes passwords or user credentials less vulnerable. The technical advantage of frequent password changes must be balanced against the effects on employee password behavior. For example, requiring frequent password changes may lead to work-arounds such as employees writing their passwords down on paper.

Finally, and most important, education is essential. Unintentional negligence remains the biggest risk; attacks often propagate through inadvertent employee behavior such as opening an e-mail attachment, clicking a link embedded in an e-mail message, or otherwise entering credentials through a phishing attack. Hospital staff may be unaware that they were targeted, and the majority of breaches are discovered after the fact.[1] Regular employee training and education should be required for all members of the health care community. People are the weakest link in the security infrastructure: our systems are only as secure as the gatekeepers who use them.

Unfortunately, no system can guarantee complete security. As long as there is value in information, there will be attacks against the systems that secure it — information systems are fundamentally vulnerable. Nevertheless, if we acknowledge the public health implications of information security, we can improve dialogue, implement necessary protections, and minimize the impact on patient care.

Disclosure forms provided by the authors are available at NEJM.org.

From Brigham and Women's Hospital and the Division of General Internal Medicine, Massachusetts General Hospital (W.J.G.), the Department of Emergency Medicine, Brigham and Women's Hospital (A.L.), Harvard Medical School (W.J.G., A.L.), and Partners Healthcare (A.F., A.L.) — all in Boston.

This article was published on July 12, 2017, at NEJM.org.

1. Ponemon Institute. Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data. May 12, 2016 (http://www.ponemon.org/blog/sixth-annual-benchmark-study-on-privacy-security-of-healthcare-data-1).

2. Nigrin DJ. When 'hacktivists' target your hospital. N Engl J Med 2014;371:393-5.

3. Healthcare IT News, HIMSS Analytics. Healthcare IT News and HIMSS Analytics quick HIT survey: Ransomware. 2016 (https://healthmanagement.org/c/it/news/ransomware-attacks-hit-three-quarters-of-hospitals-without-them-knowing).

4. Cox J. Hacker advertises slew of alleged healthcare organization records. Motherboard. June 26, 2016 (https://motherboard.vice.com/en_us/article/hacker-advertises-slew-of-alleged-healthcare-organization-records).

5. ICS-CERT. Hospira Symbiq Infusion System vulnerability. July 21, 2015 (https://ics-cert.us-cert.gov/advisories/ICSA-15-174-01).

DOI: 10.1056/NEJMp1707212