ware-laden e-mail, the hospital took the precautionary step of temporarily shutting down its entire e-mail system. The shutdown gave IT staff time to quarantine malicious e-mail and to notify staff of the absolute importance of not clicking links or opening attachments without being certain that they were safe. And although having no e-mail was a minor inconvenience for most employees (and a nice respite for some), many internal processes actually depend on e-mail for normal operations, so workarounds had to be developed.

As health care organizations push forward to further enable electronic health records (EHRs), many of which are hosted remotely, the potential effect of losing Internet connectivity is large, and the analysis required to understand that effect is complex. As an organization that achieved the highest stage (Level 7) on the Health Information Management Systems Society's Analytics Electronic Medical Record Adoption Model several years ago[1] — which indicates the degree to which we have automated our inpatient care processes — our hospital has invested substantial time and resources in putting these kinds of contingency plans and security technologies in place. For organizations just beginning their EHR journey, this advance planning and attention to information security and business continuity cannot be stressed enough, especially in this new world where a cyberattack on a hospital is possible.

Health care organizations can no longer assume that they are immune from organized attacks like the one described above. As in any other industry, in addition to safeguarding against the compromise of sensitive data, health care entities must now protect themselves against direct attacks meant to disrupt operations. In clinical settings, such attacks can clearly have adverse effects on patient care. Health care organizations should strongly consider investing the time and resources in IT security systems and operational best practices to ensure that they are prepared to endure and defend against these new threats, if and when they occur.

Disclosure forms provided by the author are available with the full text of this article at NEJM.org.

From the Information Services Department, Boston Children's Hospital; and the Department of Pediatrics, Harvard Medical School — both in Boston.

[1] Electronic Medical Record Adoption Model (EMRAM): Stage 7 case studies, Children's Hospital Boston. Chicago: HIMSS Analytics (http://www.himssanalytics.org/emram/stage7caseStudies.aspx?hospID=3).

DOI: 10.1056/NEJMp1407326

Cybersecurity in Health Care

Eric D. Perakslis, Ph.D.

Most of us are aware of cyberthreats — if not because of personal experience, then thanks to a barrage of news stories. We've read that many of our banks, credit-card companies, and favorite retailers have been hacked and that tens of millions of consumers had their personal financial information stolen during the 2013 holiday season. In addition, last year brought stories of successful cyberintrusion at the Food and Drug Administration (FDA) and of the theft of the designs of major U.S. military weapons systems by foreign governments. Health care data and infrastructure are at least as vulnerable as most financial and military data. And beyond the pecuniary, regulatory, and reputational risks associated with data and identity theft lie even graver threats to health care infrastructure and patient safety.

In a recent study, a whopping 94% of health care institutions reported having been victims of cyberattacks.[1] To date, cybercrime against health care has manifested as four specific threats: data loss, monetary theft, attacks on medical devices, and attacks on infrastructure. Some cybercriminals are motivated by financial gain, whereas others seek to obtain intellectual property or consumer information, to damage an institution's reputation, or to make a political statement through "hacktivism." The privacy and security rules put in place by the Health Insurance Portability and Accountability Act (HIPAA) have raised awareness of the importance of protecting personal health information and have provided a regulatory framework to encourage compliance — but compliance does not necessarily translate into security. The fact is that most current HIPAA protection strategies rely on standard technological methods of isolating critical data, but this recent study indicates that many attackers are bypassing these types of protections and do not require stealth techniques to do so. There is a substantial knowledge and focus gap between the technology domain and the regulatory compliance domain that needs to be closed.

Health care institutions face particularly high financial risk from data theft, owing to both their liability profile and the volume and variety of data they collect and store. Of the 16 industries studied by the Ponemon Institute, a research center focused on privacy, data protection, and information security policy, health care incurred the highest per-record cost when a data loss occurred: an estimated $233. The mean for all industries was $136 per record, with the retail industry incurring the lowest cost, at $78 per record.[2] Costs include those for legal actions, recovery, security-control investments, and extended credit-protection services for victims. If these estimated costs applied to the WellPoint data breach of 2009–2010, in which security flaws left the personal and health information of more than 600,000 health-plan enrollees openly accessible, the total cost would be in the billions — dwarfing the $2 million that WellPoint had to pay in HIPAA fines. Within the health care industry, 72% of recent malicious traffic, viruses, and similar attacks have been directed against hospitals, clinics, large group practices, and individual providers, with the remaining 28% being spread among provider organizations, health plans, pharmaceutical companies, and other entities; in other words, health care delivery is being aggressively and specifically targeted.

In addition to finding ways to protect against data theft, the health care industry must focus on the other cyberthreats: financial theft, interference with medical devices, and attacks on critical infrastructure. Financial theft often resembles data theft, and analogous protections are required. The recent theft of $1.03 million from the payroll accounts of a Washington hospital, perpetrated by hackers in Ukraine and Russia aided by more than 100 accomplices in the United States, shows how sophisticated and extensive such attacks have become.[3]

But threats to medical devices and critical infrastructure may be of even greater concern because of their potential effects on patient health and safety. Patients are especially at risk from attacks that could disrupt critical medical infrastructure, disrupt communications and services, interfere with medical devices, or alter or falsify critical data or make them unavailable. The "internet of things," which connects physical equipment, such as patient monitors, that contains sensors or actuators and is programmed electronically, has enabled remote and distributed access to many diagnostic and treatment capabilities within health care institutions, but such connectivity has also created opportunity for attacks. Since 2009, the Department of Veterans Affairs has tracked hundreds of infections of devices by computer viruses and other malicious programs. Fortunately, patient safety has not yet been compromised, but the disruption and costs to patients and providers have been substantial.[4]

A dramatic increase in cyberintrusions and attacks on medical devices has caused regulators to take notice. The FDA issued a safety communication in June 2013 entitled "Cybersecurity for Medical Devices and Hospital Networks," and a cross-agency working group involving representatives of the FDA, the Office of the National Coordinator for Health Information Technology, and the Federal Communications Commission has released a report calling for increased private-sector involvement and a risk-based regulatory framework — but does not define that framework further. Unfortunately, burdensome and slow-moving regulation could greatly increase costs and possibly obscure emerging threats. The health care community would therefore be wise to heed this call from regulators and join actively in the dialogue.

The Ponemon study suggests that organizations that focus adequately on improving their cybersecurity posture, hire and empower a chief information security officer, and build strong incidence-response capabilities can reduce their potential financial risk from data breaches by 42%. An organization's security posture encompasses a complex mix of technological, operational, and procedural elements that is often difficult to truly understand, let alone improve. It isn't always clear whether the focus at any given moment should be on modernizing technology, training personnel, providing physical security, or some combination of these aspects. None of these tasks are easy, inexpensive, or quick; prioritization and a clear strategy are essential.

An active learning approach is required to make prioritized cyberprotection strategies and tactics focused and successful. This approach requires the ability to understand the complex interplay and dynamics among outside threats, inherent vulnerabilities, specific risks, and the system's resilience, all of which must be understood in the particular context of the health care delivery setting if feasible solutions are to be found. Although we cannot predict exactly what an adversary will do, we can take control of our own environments, and we must watch potential adversaries closely.

Just as public health strategies have been developed to detect and track emerging epidemics, identify population risks and vulnerabilities, and prevent or ameliorate adverse effects, analogous approaches can be used to improve cybersecurity in health care delivery organizations. First, active and real-time surveillance and communication of emerging cyberthreats could be used to profile threats and ultimately influence public policy and prevention. Second, risk-based analysis and modeling that take into account current and possible threats, the resulting risks, and the vulnerabilities and resilience of the information system can guide policy development. Third, effective regulation may help ensure the fidelity of medical devices; finding the right balance by establishing security without creating yet another expensive and distracting set of compliance standards will require prior definition by stakeholders (patients, providers, and institutions) — perhaps in a forum hosted by the Institute of Medicine, to build on its reports on privacy and data security.[5]

The threats of cyberattack are clear and present in health care. It is time to organize, convene, and focus in a way that that truly protects our patients, providers, and institutions. Technology has unquestionably improved health care. Let's be sure that its promised benefits continue to be delivered safely.

Disclosure forms provided by the author are available with the full text of this article at NEJM.org.

From the Center for Biomedical Informatics, Countway Library of Medicine, and the Department of Pediatrics, Harvard Medical School, Boston.

1. Filkins B. SANS health care cyberthreat report: widespread compromises detected, compliance nightmare on horizon. Norse. February 2014.
2. Ponemon Institute. 2013 Cost of data breach study: global analysis. May 2013.
3. Krebs on Security. Wash. hospital hit by $1.03 million cyberheist. April 2013 (http://krebsonsecurity.com/2013/04/wash-hospital-hit-by-1-03-million-cyberheist).
4. Maron DF. A new cyber concern: hack attacks on medical devices. Scientific American. June 2013 (http://www.scientificamerican.com/article/a-new-cyber-concern-hack/).
5. National Research Council, Committee on Maintaining Privacy and Security in Health Care Applications of the National Information Infrastructure. For the record: protecting electronic health information. Washington, DC: National Academy Press, 1997.

DOI: 10.1056/NEJMp1404358

HISTORY OF MEDICINE

The Origins of Antimalarial-Drug Resistance

Randall M. Packard, Ph.D.

Related article, p. 411

Drugs have been used to treat and prevent malaria for centuries. Bark from the cinchona tree, which contained an array of alkaloids with antimalarial properties, appeared in Western therapeutics in the 17th century. One of the alkaloids, quinine, was isolated in 1820 and became the drug of choice for treating malaria until World War II, when supplies of the drug for much of the world were cut off by the Japanese occupation of cinchona-growing regions in Southeast Asia. Efforts to create alternatives to quinine led to the search for synthetic antimalarial drugs. Chloroquine, first developed in the 1930s, became the most widely used synthetic antimalarial during the 1960s and 1970s.

Although the use of antimalarial drugs has a long history, the emergence of antimalarial-drug resistance is a relatively recent phenomenon. Chloroquine-resistant forms of *Plasmodium falciparum* malaria first appeared in Thailand in 1957 (see map). They then spread through South and Southeast Asia and by the 1970s were being seen in sub-Saharan Africa and South America. The rise in chloroquine resistance contributed to a worldwide increase in malaria-related mortality, particularly in sub-Saharan Africa. In an effort to combat resistant strains, a number of alternative synthetic antimalarial drugs were deployed to both treat and prevent malaria. Among these were sulfadoxine–pyrimethamine and mefloquine.[1]

Various degrees of resistance to these replacement therapies emerged relatively quickly, though it was found that when used in combinations, these drugs could still be effective in treating malaria. The disadvantages of the new therapies were their increased cost — which made them less available to the populations that were at greatest risk — and in some cases, their adverse side effects.

It was in the context of the search for new and safer antima-