Cyber Disaster Medicine: A New Frontier for Emergency Medicine

Christian Dameff, MD;* Jennifer Farah, MD; James Killeen, MD; Theodore Chan, MD

*Corresponding Author. E-mail: cdameff@ucsd.edu, Twitter: @cdameffmd.

0196-0644/$-see front matter

https://doi.org/10.1016/j.annemergmed.2019.11.011

[Ann Emerg Med. 2020;75:642-647.]

INTRODUCTION

The technologic health care revolution has improved many elements of care, but it has also introduced unintended consequences.[1-4] As with any other complex connected electronic system, health care technology is rife with software and hardware flaws, leading to vulnerability.[5,6] The exploitation of these vulnerabilities by malicious actors has become commonplace within the health care sector and is likely to accelerate as our dependence on technology continues to increase.[7] Cybersecurity, the protection of vulnerable technology from such exploitation and attacks, is a rapidly growing and an increasingly important component of risk management across nearly every industry, and health care is no exception. The formal study of health care cybersecurity, as well as the development of expertise in its clinical implications, may prove to be a key niche for the emergency physician of the future.

TECHNOLOGIC DEPENDENCE

Modern health care systems are interconnected and interdependent technical systems and are composed of a myriad of different software, hardware, medical devices, and networking products. The interoperability, or the ability of these systems to communicate and work with one another, was required under the Meaningful Use provision of the Health Information Technology for Economic and Clinical Health act passed by Congress in 2009.[8] In 2017, the US Department of Health and Human Services released a congressionally mandated task force report stating that health care cybersecurity is in critical condition, leading many individuals to conclude that the ability to connect these systems has greatly outpaced the ability to secure them.[9]

Attacks on connected computerized systems vary greatly in influence, sophistication, and scale, often depending on the malicious actor's intent and skill. Traditionally, these attacks have been described by the "CIA triad."[10] This model groups attacks into 3 categories, confidentiality, integrity, and availability (Figure 1). Confidentiality involves the protection of data access from individuals who are not authorized. For example, if hackers exposed protected health information such as names, addresses, and medication lists of patients, it would be categorized as a confidentiality attack.[11] Integrity is the assurance that data stored or transmitted from a location remain free from unauthorized alteration. An attack that changes the values of laboratory tests in a database from abnormal to normal or erases a patient's critical drug allergies from the electronic medical record would be categorized as an integrity attack.[12] Ensuring the continued access to or preserving the function of computerized system is called availability. If a hacker launched an attack on a pharmacy system that resulted in inaccessibility to pharmacists or physicians, it would be called an availability attack.[5] Malicious actors can use these attack types singly or in combination.

Malicious computer programs known as malware have proliferated across the Internet in the past 2 decades.[13] Ransomware, programs that render data inaccessible until a financial payment has been made to the attacker, has recently infected hundreds of health care systems. Perhaps the most devastating of these incidents occurred in May 2017, when the WannaCry ransomware infected systems in greater than 80 UK National Health Service hospitals, resulting in closure of some emergency departments (EDs), cancellation of surgeries, and disruption of outpatient clinical care.[14]

Beyond malware, malicious hackers can launch digital attacks targeting the theft of protected health information. In 2017 alone, 5.6 million patient records from 477 breaches were known to be compromised in the United States.[15] These records contain all the necessary information to perform identity and financial theft, and

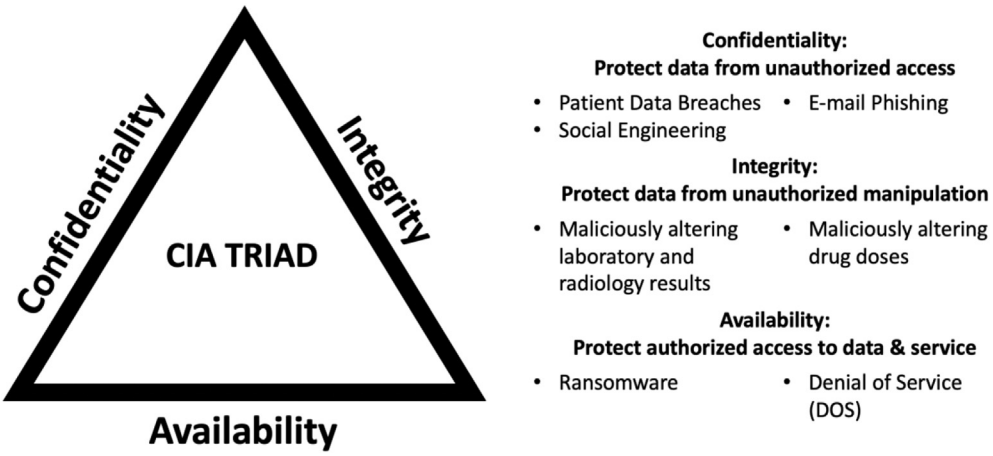

Figure 1. Cybersecurity attack classification with health care examples.

contain potentially sensitive medical information (such as HIV status) that can be leveraged for patient blackmail. Despite significant resource allocation to this problem, breaches continue to pose a significant legal and financial liability to health care delivery organizations.

Many connected medical systems are vital for the clinical treatment work flows of time-dependent medical conditions such as stroke, trauma, cardiac arrest, and sepsis (Figure 2). The failure of even one of these systems may produce an adverse outcome for a patient. For example, although it has not been reported, failure of a computed tomography (CT) scanner's operating system because of a computer virus may prolong the diagnosis of stroke, pushing the patient outside the thrombolytic treatment window or delaying neurosurgical intervention of an intracranial hemorrhage. Even technical system failure outside the digital borders of a hospital can affect patient care, as was exemplified by the 2018 Allscripts ransomware attack that left hundreds of infected hospitals and clinics without the ability to view patient records or prescribe medications because of Allscripts' security breach.[16]

Hospitals also deploy vast networks of connected devices and systems that can affect clinical care even though they are not traditionally thought of as clinical in nature. For example, a denial-of-service attack on a hospital paging or telephone system may delay specialist intervention in ST-segment elevation myocardial infarction and trauma work flows, in which rapid communication is vital. Furthermore, attacks on critical hospital facility infrastructure such as electrical grids or water supply can affect clinical care.[17]

Medical devices can be especially difficult to secure and pose direct patient care effects. They can take years from

Diagnostic	Treatment	Support	Information
Laboratory devices	**Implantables**	**Facilities**	Electronic health records
Chemistry	Pacemakers	Elevators	
Hematology	Neuromodulators	Electricity supply	
Pathology	Patient-controlled analgesia	Water supply	
		Heating, ventilation, and air conditioning systems	
Radiographic devices	**Medication delivery**	**Communications**	Health information exchanges
Radiographs	Infusion pumps	Radio systems	
CT scanners	Insulin pumps	Internet connectivity	
MRI machines	Medication storage	Paging systems	
Ultrasonography	Pharmacy delivery		
ECG machines	**Organ replacement**	**Monitoring**	
	Ventilators	Telemetry	
	Dialysis machines		
	Bypass machines		

MRI, Magnetic resonance imaging.

Figure 2. Potentially vulnerable connected medical devices and systems.

inception to final Food and Drug Administration approval, often containing antiquated software and vulnerable legacy operating systems that were state of the art when these devices were initially designed. In recent years, the Food and Drug Administration has published several resources in regard to medical device cybersecurity development best practices as well as support for securing current devices in clinical use.[18,19]

The increasing reliance on connected technical systems and electronic medical records in health care has increased the risks of these types of attacks and other cybersecurity vulnerabilities. When these systems are compromised, the effects can subsequently resemble those of other disasters or mass casualty events, in which damaged infrastructure significantly affects the delivery of clinical care. The ease by which these attacks scale, as well as their potential to disrupt care, has drawn comparison to natural disasters such as hurricanes and earthquakes.

CYBER DISASTER MEDICINE

The preparation for and medical management of natural disasters, disease outbreaks, and mass casualty incidents are among the primary responsibilities of emergency medicine and its subspecialty disaster medicine. Formalized fellowship training in disaster medicine has existed for decades and continues to be a desirable subspecialization among graduating emergency medicine trainees. Disaster planning and preparedness is a requirement for hospital accreditation by The Joint Commission (TJC), and best practices are studied and published in the academic literature.[20] An essential component of resilient health care systems and a key practice of disaster medicine is the proactive surveillance for emerging threats that have the potential to disrupt the delivery of care on a large scale.

Cyber attacks do not follow a predictable pattern for initial infection or progression, often spreading indiscriminately at the speed of broadband Internet. Many natural disasters such as hurricanes or earthquakes have a geographic predilection and a historical precedent, allowing hospitals in certain regions to prepare for and test robust disaster response plans. Conversely, malware or other cyber attacks can strike anywhere there is Internet connectivity, affecting regions that may traditionally have been isolated from any type of disaster. The risk of rapid spread from one hospital to another means a single infection can quickly infect a whole health care system, rapidly decimating clinical care capabilities among dozens of hospitals.[14,21] Furthermore, defenses from cyber attacks often require sophisticated and costly security systems. Critical-access hospitals and resource-scarce health care delivery systems that have not invested in secure infrastructure are at particular risk, increasing the potential of such attacks to disproportionately affect impoverished and underserved communities.

Formalized management of these health care cyber attacks is in its infancy and will require the application of traditional disaster medicine principles, as well as novel strategies, because of the unique nature of these new threats. Developing cyber disaster best practices and formalized training in emergency medicine should be a priority and built with the support of national and regional disaster agencies. The Federal Emergency Management Agency has traditionally been the beacon for outlining disaster management practices. More specifically, their model of the incident command system is commonly taught during emergency medicine residency and most certainly during a disaster medicine fellowship.[22] The incident command system provides a standardized management tool for meeting the specific demands related to a disaster. It outlines the leadership structure, division of labor, and responsibilities therein for all of the major components of disaster response, such as operations, planning, logistics, and finance. Although very much applicable to natural disasters (eg, earthquakes, wildfires, hurricanes) or acts of terrorism (eg, mass shooting, bombings), this model is limited in its ability to effectively manage a cyber attack. The challenges of addressing technology defects while trying to avoid disruptions in patient care are indeed unique. The development of standardized best practices for responding to cyber disasters will likely require a hybrid approach, leveraging tools of traditional emergency management incident command systems with the incident response playbooks commonly deployed by hospital information technology and information systems teams.

The common practice of an organized disaster response is to quickly dispatch as many trained professionals as possible and provide them with specific tasks. However, in the case of a cyber attack, the resource needs are very different. Rather than emphasizing manpower and supplies to meet increased patient demand, the problems most likely to ensue will require informatics specialists and pretrained individuals prepared to implement alternative, noncomputerized systems for maintaining patient flow and treatment. This requires a specialized disaster plan that does not exactly fit into the framework of the Federal Emergency Management Agency's incident command system. Therefore, emergency medicine educators should seek to create cyber-attack plans that can be incorporated as a unique hazard into a hospital's emergency operation plan.

Hospitals can implement the principles of the Federal Emergency Management Agency's phases of emergency management in the mitigation, preparedness, response, and

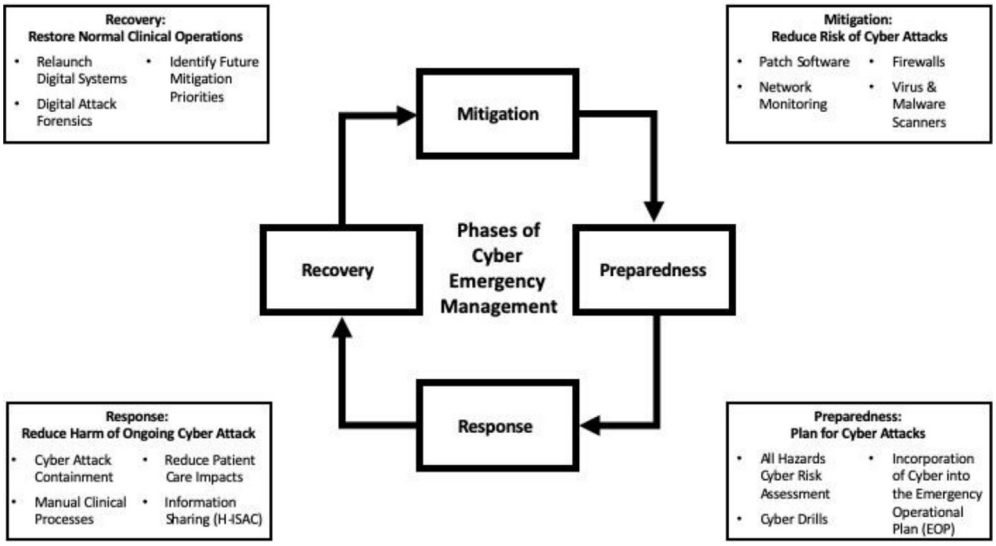

Figure 3. Phases of cyber emergency management.

recovery of cyber attacks on health care (Figure 3). Mitigation strategies of these attacks primarily fall under the information technology department of hospitals and should follow industry best practice standards such as those of the National Institute of Standards and Technology.[23] Involvement of clinicians in the mitigation process can also improve the security posture of health care in identifying the highest-priority clinical systems and devices to focus limited resources in securing. Physicians should also prioritize security as well as clinical features in device procurement recommendations, thus introducing more resilient systems into the clinical environment from the start.

Preparedness should involve the information technology departments as well as emergency management, working closely together to harmonize information technology's incident response and traditional health care incident command, avoiding siloed, duplicative response during an actual disaster.[24] Furthermore, sustained representation from information technology on all disaster hazard planning efforts would likely improve responses to technical and nontechnical disasters alike, given that many disasters affect technical systems and subsequent clinical work flows.

Real-time response to cyber disasters requires unique procedures from other disaster responses, and generally involves 3 objectives. The first is to replace digital clinical work flows with manual processes to ensure continued safe clinical care. The well-publicized failure of Beth Israel's hospital computer systems in 2002 highlighted the necessity for robust and rigorously tested information technology failure procedures.[25] The second objective is to identify the specific cyber threat and limit its spread and effect on the network. The third objective is to contact relevant external agencies and organizations such as the Federal Bureau of Investigation, Department of Homeland Security, and other health care entities through the privileged Health Information Sharing and Analysis system.

Recovering from medical cyber disasters also requires some unique considerations. While relaunching clinical systems affected by the attack, information technology teams will need to ensure that the vulnerabilities that allowed the attacks are patched; otherwise, the same virus, malware, or attacker who exploited the system can return as soon as the systems are relaunched. Furthermore, heightened monitoring of the network for subsequent attacks as well as the identification of alternate security vulnerabilities should be a priority.

TJC requires that health care organizations test their disaster plan at least twice a year.[20] Many physicians are familiar with these drills because they are commonly asked to participate in triaging mock patients. The exercise of triaging is most commonly performed in the context of an influx of patients that stems from a natural disaster. During this scenario, a physician may be asked to improvise techniques to triage and treat patients. But what if the disaster is not an influx of patients, but rather the complete absence of any electronic forms of communication, patient tracking, or ordering of diagnostic tests? Instead of a technology failure's being the temporary adverse effect of a natural disaster, what if it *were* the disaster? Anyone who has experienced a downtime of a hospital's electronic medical record system is familiar with this vulnerable state. And yet how often is this scenario applied to disaster drills? Downtime itself may be the only time to realistically simulate a cyber disaster. Efforts to practice and refine manual patient care processes can be added to these downtimes.

In 2017, the Healthcare Information and Management Systems Society conducted a survey of 126 information security professionals from a variety of US health care organizations.[26] This survey explored topics in cybersecurity, such as frequency of emergency drills, nature of incident response policies, and fund allocation. It revealed that a large percentage (40% to 60%) of these health care organizations do not conduct mock exercises to test for failure of technology resources. Unfortunately, this survey further illuminates the lack of preparation of many health care institutions for a cyber disaster.

Residents offer a unique perspective to this risk. Traditionally coming from a younger generation than their predecessors, residents often are better versed in technology than their attending physicians.[27] However, this exposure also predisposes residents to a potential dependence on computerized systems because they likely never have had to function in a hospital that solely relies on paper, let alone during a disaster. Thus, residents embody an interesting duality: increased knowledge of technology (and risks therein) coupled with a need to familiarize themselves with noncomputerized hospital systems. Therefore, residents are the ideal population to be at the forefront of cyber disaster preparedness.

This call to action is congruent with existing resident education practices. As is well known in emergency medicine residency training, the Accreditation Council for Graduate Medical Education, in conjunction with the American Board of Emergency Medicine, has created milestones for emergency medicine education.[28] It offers an outline for categorizing levels of competency throughout the course of a resident's training. Included in these milestones are performing improvement projects for patient safety (milestone 16), demonstrating an awareness of the larger context of health care (milestone 17), and using technology to accomplish safe health care delivery (milestone 18). Thus, having residents design and partake in technology-related disaster drills assists in achieving these milestones.

RECOMMENDATIONS

Mandating intensive technical cybersecurity disaster training for every emergency physician is not feasible nor a tremendously beneficial use of limited physician resources. However, department leadership and disaster-oriented physicians can lead cyber disaster preparedness efforts. We propose specific recommendations for emergency physicians for cyber disaster preparedness. The first thing to implement is regular ED and hospitalwide cyber disaster drills, simulating a technical failure of all digital systems. An even easier way to accomplish this task is to use your institution's next scheduled electronic health record downtimes to practice effective nondigital patient care procedures. Members of your information technology and information services teams should participate in the crafting of these drills as well. To further accelerate your preparedness goals, introduce and develop a cyber disaster task force that includes technical, clinical, and organizational leadership. You then can share best practices with other health care delivery organizations. If and when a cybersecurity threat affects your hospital, participate in health care interorganizational threat sharing by using existing international mechanisms, such as the Health Information Sharing and Analysis Center. And finally, some of the simplest ways an emergency physician can safeguard his or her hospital from a cyber threat is to practice good cyber hygiene.[24]

- Create longer unique pass phrases instead of a password found in dictionaries.
- Do not share passwords or pass phrases.
- Avoid using the same password or pass phrase for multiple accounts and services.
- Avoid sharing information on social media that can be used to answer security questions.
- Deploy multifactor authentication.
- Avoid accessing clinical systems from untrusted environments such as coffee shops and airports.
- Avoid opening malicious e-mails.
- Avoid connecting rogue flash drives to clinical environments.
- Encrypt digital data storage.
- Avoid disclosing sensitive information to unverified persons who may be impersonating authorized users.

CONCLUSION

As health care technology systems increase in sophistication, so does their vulnerability to cyber attacks. Emergency medicine is particularly susceptible to this threat, given the medical safety-net nature of practice, because emergency care is unable to be suspended while damaged systems await repair. However, emergency medicine also has the advantage of an extensive history of disaster management expertise and thus can serve as a leader for its hospital's cyber disaster response. More specifically, emergency medicine residents and other trainees can capitalize on their more advanced knowledge of computer systems to spearhead development of cyber medical disaster preparedness efforts. Governmental agencies, policymakers, and health care delivery organizations should allocate resources to formally study this phenomenon. Disaster medicine fellowship programs should incorporate cyber disaster response into training, and emergency medicine specialty organizations such as the American College of Emergency Physicians (ACEP) should

support efforts to improve health care cybersecurity resilience internationally. These measures will ensure the continued development of cyber medical disaster response and will save patient lives.

Supervising editors: Joshua Mirkin, MD; Jason D. Heiner, MD. Specific detailed information about possible conflict of interest for individual editors is available at https://www.annemergmed.com/editors.

Author affiliations: From the Department of Emergency Medicine (Dameff, Farah, Killeen, Chan), Department of Biomedical Informatics (Dameff), and the Department of Computer Science and Engineering (Dameff), University of California–San Diego, San Diego, CA.

Authorship: All authors attest to meeting the four ICMJE.org authorship criteria: (1) Substantial contributions to the conception or design of the work; or the acquisition, analysis, or interpretation of data for the work; AND (2) Drafting the work or revising it critically for important intellectual content; AND (3) Final approval of the version to be published; AND (4) Agreement to be accountable for all aspects of the work in ensuring that questions related to the accuracy or integrity of any part of the work are appropriately investigated and resolved.

Funding and support: By *Annals* policy, all authors are required to disclose any and all commercial, financial, and other relationships in any way related to the subject of this article as per ICMJE conflict of interest guidelines (see www.icmje.org). Dr. Farah is a paid contributor to Emergency Medicine: Reviews & Perspectives (EM:RAP).

REFERENCES

1. Clarke R, Youngstein T. Cyberattack on Britain's National Health Service: a wake-up call for modern medicine. *N Engl J Med*. 2017;377:409-411.
2. Buntin MB, Burke MF, Hoaglin MC, et al. The benefits of health information technology: a review of the recent literature shows predominantly positive results. *Health Aff (Millwood)*. 2011;30:464-471.
3. del Carmen MG, Herman J, Rao S, et al. Trends and factors associated with physician burnout at a multispecialty academic faculty practice organization. *JAMA Netw Open*. 2019;2:e190554.
4. Rahurkar S, Vest JR, Menachemi N. Despite the spread of health information exchange, there is little evidence of its impact on cost, use, and quality of care. *Health Aff (Millwood)*. 2015;34:477-483.
5. Nigrin DJ. When "hacktivists" target your hospital. *N Engl J Med*. 2014;371:393-395.
6. Halperin D, Benjamin TS, Ransford B, et al. Pacemakers and implantable cardiac defibrillators: software radio attacks and zero-power defenses. 2008. Available at: https://ieeexplore.ieee.org/document/4531149. Accessed January 7, 2020.
7. Gordon WJ, Wright A, Aiyagari R, et al. Assessment of employee susceptibility to phishing attacks at US health care institutions. *JAMA Netw Open*. 2019;2:e190393.
8. Blumenthal D. Launching HITECH. *N Engl J Med*. 2010;362:382-385.
9. Health Care Industry Cybersecurity Task Force. Report on Improving Cybersecurity in the Health Care Industry. June 2017. Available at: https://www.phe.gov/preparedness/planning/cybertf/documents/report2017.pdf. Accessed June 21, 2019.
10. Schabacker DS, Levy L-A, Evans NJ, et al. Assessing cyberbiosecurity vulnerabilities and infrastructure resilience. *Front Bioeng Biotechnol*. 2019;7:61.
11. Jiang JX, Bai G. Evaluation of causes of protected health information breaches. *JAMA Intern Med*. 2019;179:265-267.
12. Zetter K. Hospital viruses: fake cancerous nodes in CT scans, created by malware, trick radiologists. Available at: https://www.washingtonpost.com/technology/2019/04/03/hospital-viruses-fake-cancerous-nodes-ct-scans-created-by-malware-trick-radiologists/. Published April 3, 2019. Accessed June 21, 2019.
13. Gordon WJ, Fairhall A, Landman A. Threats to information security—public health implications. *N Engl J Med*. 2017;377:707-709.
14. National Audit Office. Investigation: WannaCry cyber attack and the NHS—National Audit Office (NAO) report. Available at: https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/. Accessed June 21, 2019.
15. Spitzer J. 5.6M patient records breached in 2017: 6 things to know. Available at: https://www.beckershospitalreview.com/cybersecurity/5-6m-patient-records-breached-in-2017-6-things-to-know.html. Accessed June 21, 2019.
16. Healthcare IT News. Allscripts sued over ransomware attack, accused of "wanton" disregard. Available at: https://www.healthcareitnews.com/news/allscripts-sued-over-ransomware-attack-accused-wanton-disregard. Accessed June 21, 2019.
17. Wired. The highly dangerous "Triton" hackers have probed the US grid. Available at: https://www.wired.com/story/triton-hackers-scan-us-power-grid/. Accessed June 21, 2019.
18. FDA Center for Devices and Radiological Health (CDRH). Content of premarket submissions for management of cybersecurity in medical devices. Available at: https://www.fda.gov/media/119805/download. Accessed June 21, 2019.
19. Food and Drug Administration. Postmarket management of cybersecurity in medical devices. Available at: https://www.fda.gov/media/95862/download. Accessed June 21, 2019.
20. Joint Commission. Emergent management standards supporting collaboration planning. Available at: https://www.jointcommission.org/assets/1/6/EM_Stds_Collaboration_2016.pdf. Accessed June 21, 2019.
21. Collier R. NHS ransomware attack spreads worldwide. *CMAJ*. 2017;189:E786-E787.
22. Rimstad R, Braut GS. Literature review on medical incident command. *Prehosp Disaster Med*. 2015;30:205-215.
23. National Institute of Standards and Technology (NIST). Framework for improving critical infrastructure cybersecurity. Available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. Accessed June 21, 2019.
24. Dameff C, Pugh J. What to do when cyber attack strikes the emergency department. Available at: https://www.acepnow.com/article/cyber-attack-strikes-emergency-department/. Accessed June 21, 2019.
25. Kilbridge P. Computer crash—lessons from a system failure. *N Engl J Med*. 2003;348:881-882.
26. Healthcare Information and Management Systems Society. 2018 HIMSS cybersecurity survey. Available at: https://www.himss.org/sites/himssorg/files/u132196/2018_HIMSS_Cybersecurity_Survey_Final_Report.pdf. Accessed June 21, 2019.
27. Jingjing J. Millennials stand out for their technology use. Available at: https://www.pewresearch.org/fact-tank/2018/05/02/millennials-stand-out-for-their-technology-use-but-older-generations-also-embrace-digital-life/. Accessed June 21, 2019.
28. Accreditation Council for Graduate Medical Education. Emergency Medicine Milestone Project. Available at: https://www.acgme.org/Portals/0/PDFs/Milestones/EmergencyMedicineMilestones.pdf. Accessed June 21, 2019.