Technology in Anesthesiology: Opportunities for Innovation

Formation of an ASA Cybersecurity Task Force (CSTF) to Protect Patient Safety

Julian M. Goldman, MD Beth Minzter, MD, MS, FIPP Jaime Ortiz, MD, MBA, FASA Mark Banoub, MD, FASA, MBA, CPE, FASA, FAAPL Brian Rothman, MD

Julian M. Goldman, MD
Committee on Electronic Media and Information Technology, and Medical Director, Partners HealthCare Biomedical Engineering, Assistant in Anesthesia, Massachusetts General Hospital/ HMS, Director, Medical Device Interoperability Program (MD PnP) at MGH/PHS, Boston.

Beth Minzter, MD, MS, FIPP
Committee on Electronic Media and Information Technology, and Quality Improvement Officer, Department of Pain Management; Medical Director, Main Campus Pain Management, Cleveland Clinic.

Jaime Ortiz, MD, MBA, FASA
Committee on Electronic Media and Information Technology, and Associate Professor of Anesthesiology, Baylor College of Medicine; Deputy Chief of Anesthesiology Service, Director of Regional Anesthesia, and Co-Director Acute Pain Management Service, Ben Taub Hospital, Houston.

Mark Banoub, MD, FASA, MBA, CPE, FASA, FAAPL
Committee on Electronic Media and Information Technology, and Senior Staff Anesthesiologist, Henry Ford Medical Group.

Brian S. Rothman, MD
Chair, Committee on Electronic Media and Information Technology, Associate Professor of Anesthesiology, Surgery, and Biomedical Informatics, and Medical Director, VUMC Revenue Cycle, Vanderbilt University School of Medicine, Nashville.

Anesthesiologists and the lay public are familiar with ransomware attacks of electronic health records (EHRs) in which EHR databases are encrypted until a ransom is paid. But the EHR is not the only vulnerable perioperative equipment. Medical devices may be susceptible to cybersecurity threats.

Over the last two years, software vulnerabilities that render specific models of anesthesia workstations, ventilators, infusion pumps, and imaging devices susceptible to cybersecurity attacks have been identified.

Examples of effects of cybersecurity attacks on medical devices:

- shutdown of device
- distortion of display screen
- loss of device functions
- over or under delivery of tidal volume
- inaccurate data presented on a remote alarm display
- erroneous data transmitted to the EHR
- remote control of device settings
- silencing of alarms
- theft of patient data
- inability to update IV drug library

If one of these software vulnerabilities is exploited through a nefarious attack, device performance could be affected in diverse and subtle ways that may be difficult to detect during clinical care.

Intrinsic to the safe conduct of anesthesia is the assessment of risks and implementation of appropriate mitigation plans. For example, we perform pre-use equipment checks and plan for foreseeable equipment failures by ensuring the availability of a secondary oxygen supply, manual self-inflating resuscitator, and a flashlight for every anesthetic. If an event and its clinical impact are foreseeable, we plan accordingly.

Are the clinical implications of cybersecurity threats foreseeable?

In view of the diversity of cyberattacks, analysis of how an attack may affect medical device performance and patient care, and what specific clinical and technical risk mitigation strategies are necessary to protect our patients, is a significant challenge.

Furthermore, the medical device may not have been intentionally attacked – it may fail as a result of "collateral damage" of an electronic medical record (EMR) attack. The attacker may not have intended for the malware to attack medical devices that are on the same network as the EMR and may have no idea if and how the medical devices will be affected.

The current generation of medical devices are considered "legacy" equipment because they were not typically designed with cybersecurity in mind. Unlike computers and smart phones, software upgrades to mitigate cybersecurity vulnerabilities may be difficult or impossible to deploy. Therefore, we must be prepared for a long transition to more secure and maintainable products.

In view of the continuing emergence of medical device cybersecurity issues, what could be done?

The U.S. FDA has developed pre- and post-market cybersecurity guidance (www.fda.gov/medical-devices/digital-health/cybersecurity). Manufacturers have been directed by the FDA to be more transparent about any vulnerability that could result in clinical impact and the risk mitigation process. ASA members have participated in FDA-led projects on medical device cybersecurity preparedness and response.

One challenge to achieving better cybersecurity is that manufacturers perform cybersecurity clinical hazard analyses with limited information from a diversity of clinicians and practice environments. Consequently, manufacturers may not perceive the clinical impact of the threat or of the recommended mitigation.

Examples of clinical risk assessment that may be performed by a manufacturer or hospital: If a cybersecurity attack could remotely silence a device's alarm, is that a clinically significant risk? Should the device be removed from service until a software patch is available? We may agree that the answer depends on the clinical need to use the device, the specific alarm affected, and the practice environment. If the audible alarm could be deactivated by the attack, perhaps we would keep the device in service if the alarm is normally turned off when the device is in use. Or we may choose to remove the device from service if the alarm is a critical safety feature in that practice setting.

Public confidence in anesthetic care could be eroded by ongoing media reports of cybersecurity threats and should be proactively addressed by ASA for the benefit of our members and our patients. Consequently, at the October 2019 meeting of the Committee on Electronic Media and Information Technology (EMIT), it was proposed to establish a Cybersecurity Task Force (CSTF) within the committee with the following objectives:

- Provide cross-functional expert risk-assessment and mitigation guidance of cybersecurity threats to perioperative medical device systems on an ongoing and emergency response basis.
- Provide guidance to ASA leadership and membership to improve general cybersecurity preparedness, including possible practice refinements such as
  - Addition of cybersecurity-related equipment failures in differential diagnosis considerations
  - Updated equipment procurement language that may reduce device vulnerabilities

The CSTF proposes to liaise with experts in the FDA, the ASA Committee on Equipment and Facilities, the APSF Committee on Technology, the Society for Technology in Anesthesia, and standards bodies such as ISO Technical Committee 121, IEC 62, AAMI A/R, and UL, to reach technical and clinical subject matter experts. In addition, the CSTF could collaborate with labs that test and evaluate cybersecurity solutions to facilitate sharing the results with hospitals for implementation. ■