Can J Anesth/J Can Anesth (2021) 68:1838–1839
https://doi.org/10.1007/s12630-021-02102-2

CORRESPONDENCE

Intraoperative cyberattacks: cyberthreat awareness and cyber-resilience strategies in anesthesia

Joseph C. Goldstein · **Heidi V. Goldstein**

Received: 24 August 2021 / Revised: 24 August 2021 / Accepted: 25 August 2021 / Published online: 7 September 2021

Keywords cybersecurity · cyberattack · resilience · pandemic · simulation

To the Editor,

Cyberattacks have been on the rise for many years, and the global cost of cybercrime is now estimated to exceed one trillion US dollars annually.[1] The extent of malicious cyber campaigns during the COVID-19 outbreak prompted the cybersecurity agencies of the United Kingdom and United States to issue a joint cyber warning in 2020.[2]

Cybersecurity concerns in healthcare tend to revolve around the impact on electronic health record systems. We would like to bring attention to easily overlooked, yet potentially serious cyber-vulnerabilities of essential anesthesia devices.

In 2019, widely used anesthesia machine models were found to be exploitable, theoretically allowing "*an attacker the ability to remotely modify (…) anesthesia device parameters*".[3] And certain commonly used infusion pumps were discovered to "*allow unauthorized arbitrary code execution*".[4] Just last year, it was revealed that vital sign monitors of a major manufacturer could "*allow an attacker access to administrative controls and system configurations*".[5]

The above examples with their associated safety advisories represent three device groups that are at the core of our anesthetic practice. Hence, it is conceivable that a cybersecurity incident renders anesthesia systems useless, comparable to how a ransomware attack locks end-users out of their computers. A much less likely, but more sinister targeted attack would be one that purposefully falsifies vital sign monitoring data in a way that intraoperative occurrences of, for instance, hypotension, arrythmias or desaturations would be concealed by displaying normal vital signs (or vice versa), resulting in improper decision-making. Ventilator settings could be changed to deliver deleterious tidal volumes, airway pressures, gas concentrations, or other harmful combinations, while presenting expected values to the observer. Infusion pump systems could be hacked to deliver inappropriate dosages while simultaneously disguising this by altering the screen output.

The fact that above illustrations seem mostly speculative at this point should not make us complacent. The advisories by the US Cybersecurity and Infrastructure Security Agency (CISA)[3–5] make it clear that such cyberattacks could indeed reach patients under anesthesia. Being prepared for rare and unexpected events is at the core of our specialty and consequently it seems prudent to raise awareness and discuss resilience strategies. A feasible option would be to approach this through simulation exercises. Many practices already conduct drills for rare clinical crises that benefit from periodic rehearsal such as malignant hyperthermia or operating room fire scenarios. Cyberattack events would

J. C. Goldstein (✉)
Department of Anesthesiology, North Florida/South Georgia Veterans Health System and the University of Florida, Gainesville, USA
e-mail: cgoldstein@anest.ufl.edu

College of Medicine, University of Central Florida, Orlando, FL, USA

H. V. Goldstein
Department of Anesthesiology, North Florida/South Georgia Veterans Health System and the University of Florida, Gainesville, USA

fit well into this category and adding cyber-resilience training to pre-existing simulation sessions should be possible without being cost or time prohibitive. The core strategies to mitigate an intraoperative cyber-strike—should the usual network defenses and computer safety measures fail—are familiar to anesthesiologists: the steps mirror the responses to device failures. Backup or transport devices that are not connected to a computer network can be used as alternatives. Simple self-inflating manual resuscitators or gas-driven pneumatic transport ventilators can act as ventilator substitutes. Transport monitors can be deployed to temporarily replace affected main vital sign monitors. Manual blood pressure cuff measurements can be used to double-check automated blood pressure devices, and clinical observation should complement one's monitoring strategies. Non-networked transport infusion pumps are also available in many centres, allowing continuation of intravenous anesthesia delivery and other important infusion therapies. Lastly, electronic health record and anesthesia record keeping system outages should be mitigated by following usual downtime contingency protocols (i.e., paper charting).

Perioperative services should already have reasonable device and power failure mitigation measures in place. The proposed addition of cyberattack training to existing simulation drills would not only educate staff about possible threats and how to mitigate them but also emphasize the necessity of best cybersecurity practices to protect vulnerable anesthesia systems from malware infection and intrusion. As vigilant anesthesiologists practicing in an era of increasing cyberattacks, we should become cyberthreat aware and cyber-resilient for the safety of the patients entrusted to us.

Disclosures None.

Funding statement None.

Editorial responsibility This submission was handled by Dr. Philip M. Jones, Deputy Editor-in-Chief, *Canadian Journal of Anesthesia/ Journal canadien d'anesthésie.*

References

1. *McAfee.* The Hidden Costs of Cybercrime. Available from URL: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf (accessed August 2021).
2. *US Cybersecurity and Infrastructure Security Agency (CISA).* Cyber Warning Issued for Key Healthcare Organizations in UK and USA. Available from URL: https://www.cisa.gov/news/2020/05/05/cyber-warning-issued-key-healthcare-organizations-uk-and-usa (accessed August 2021).
3. *US Cybersecurity and Infrastructure Security Agency (CISA).* GE Aestiva and Aespire Anesthesia (Update A). Available from URL: https://us-cert.cisa.gov/ics/advisories/icsma-19-190-01 (accessed August 2021).
4. *US Cybersecurity and Infrastructure Security Agency (CISA).* BD Alaris Gateway Workstation. Available from URL: https://us-cert.cisa.gov/ics/advisories/ICSMA-19-164-01 (accessed August 2021).
5. *US Cybersecurity and Infrastructure Security Agency (CISA).* Philips SureSigns VS4. Available from URL: https://us-cert.cisa.gov/ics/advisories/icsma-20-233-01 (accessed August 2021).