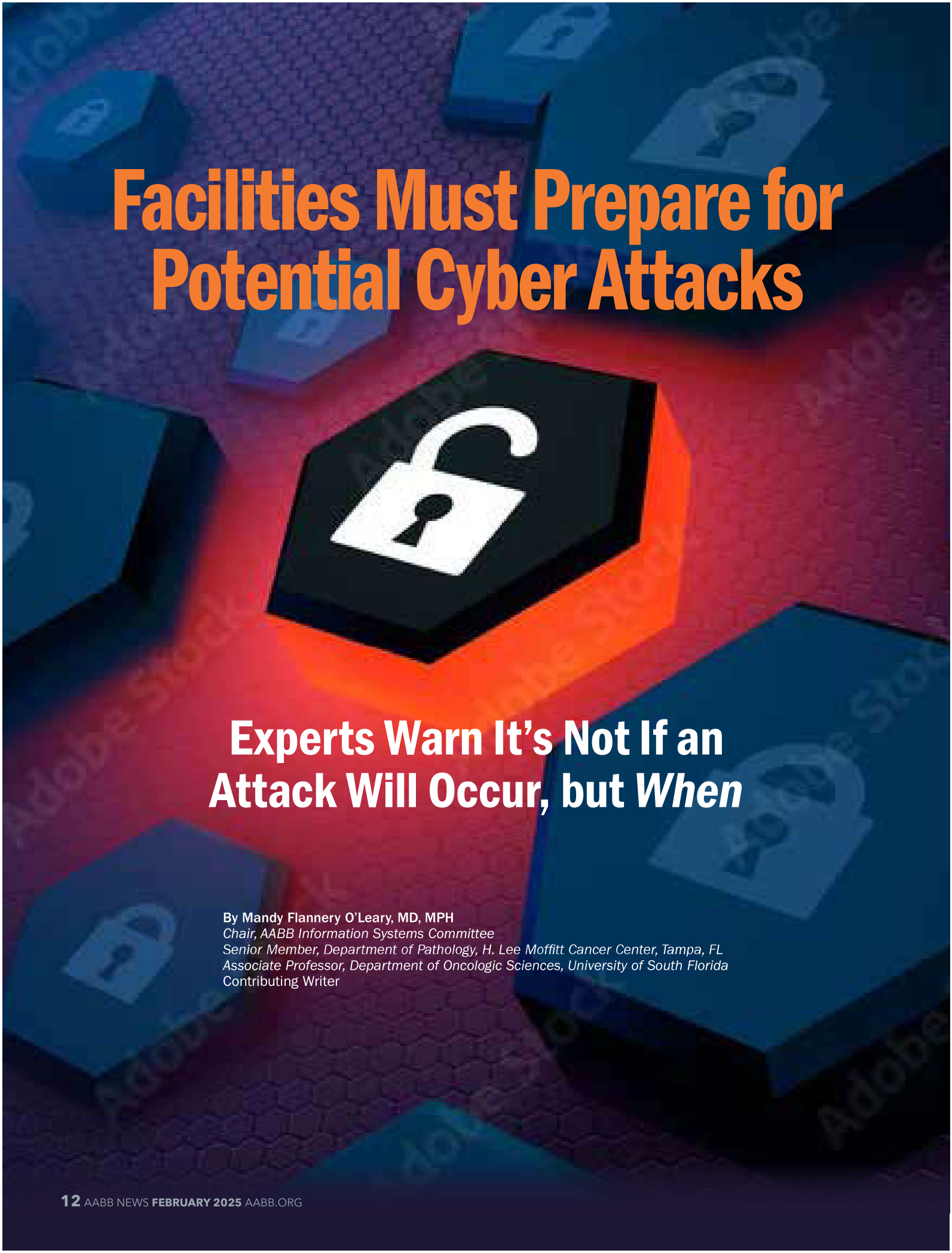
Facilities Must Prepare for Potential Cyber Attacks



Experts Warn It's Not If an Attack Will Occur, but *When*

By Mandy Flannery O'Leary, MD, MPH
Chair, AABB Information Systems Committee
Senior Member, Department of Pathology, H. Lee Moffitt Cancer Center, Tampa, FL
Associate Professor, Department of Oncologic Sciences, University of South Florida
Contributing Writer

Fall 2024 was, unfortunately, a disaster-heavy time for Florida, with hurricanes Debby, Helene and Milton hitting the state within a two-month span. Also, one of the area's major blood suppliers, OneBlood, was the victim of a cybersecurity attack.

With the increase in the number of cyberattacks recently in health care facilities, AABB leadership showed commitment to keeping our blood supply safe in the evolving digital world. The Association organized the AABB Executive Cybersecurity Summit program, held in conjunction with the 2024 AABB Annual Meeting, with key leaders from government, private health sectors, blood centers, IT and hospitals. Attendees reviewed the latest information about cyberattacks and preparedness, as everyone agreed it would not be a matter of if others would be attacked, but *when*. AABB leadership worked with DigiTRAX as a sponsor to make the summit's recording available to members (scan the QR Code at the end of this article to view the recording). The key takeaway points on recent cyber threats and preparedness are summarized for you in this article.

Key Highlight: Cybersecurity Challenges and Strategies for Health Care Facilities

The summit consisted of three panels of speakers, moderated by Dave Green, CEO of Vitalant. Green expressed the importance of the meeting, noting that his own center had recently survived multiple cyberattacks. The panels respectively focused on three topics: 1) cybersecurity challenges and strategies in health care; 2) transfusion medicine and blood banking lessons learned from recent cybersecurity breaches throughout the world; and 3) opportunities for improvement in safety of the blood supply chain regarding cybersecurity efforts.

The first panel consisted of cybersecurity leaders from the U.S. government and health sectors who addressed current cybersecurity challenges and possible abatement strategies. CDR Thomas Cristl, director of the Office of Critical Infrastructure Protection with the Administration for Strategic Preparedness and Response (ASPR), discussed recent updates in cybersecurity in the health care and public health sector from the U.S. Department of Health and Human Services (DHHS). Zach Nelson, CISSP, GSOM, GCTI, vice president of the Threat Operations Center for Health-ISAC (Health Information Sharing and Analysis Center), discussed information sharing to increase health sector resilience (ability to operate in times of cyberattack) in mitigating blood supply chain threats. George Reeves, the supervisory cybersecurity advisor at Cybersecurity & Infrastructure Security Agency (CISA), Region VI - South Texas & New Mexico, talked about government resources from CISA and how to leverage them. Collectively, these experts discussed the increase in number, type and severity of cyberattacks, especially in health care.

A major challenge is that cyber criminals are getting smarter, attacking strategic partners of hospitals in addition to directly targeting hospitals themselves. This includes facilities involved in the blood supply chain, so these cybersecurity issues are patient safety issues. The speakers' ask of AABB is to engage with

caption

their departments to increase coordination and communication for cybersecurity in blood banking.

ASPR has been focused recently on cybersecurity and has worked with CISA and the FBI. Its leaders have helped create a partnership between the government coordinating councils including CISA and private health sector councils like Health-ISAC to jointly strategize in identifying and helping address and inform consensus policy around cyber threats.

The DHHS has worked with and through these groups toward cybersecurity measures in health care by creating Cybersecurity Performance Goals (CPGs) that provide best-practice guidance to health care and public health organizations about recommended cybersecurity controls to improve cyber preparedness and resilience and protect patient safety. To help identify organizational risk and develop cyber preparedness plans, AABB members were urged to contact, and work with, CISA to maintain resiliency, as this group can provide facilities with

assistance with cybersecurity assessments and vulnerability scanning services.

Key Highlight: Lessons Learned from Cybersecurity Breaches

During the summit's second panel, participants shared their recent experiences with cyberattacks and insights on how to better prepare to respond to such incidents in the future. Susan Robinson, MBBS, MRCP, MSc, MDRes, FRCP, FRCPath, from Guy's and St. Thomas' National Health Service Foundation Trust in England, shared the impact of a 2024 ransomware attack that disabled key pathology systems and required 122 days to replace their transfusion system. She emphasized the importance of coordination with outside entities and highlighted the lack of resilience in her facility's system, combined with the challenge of low availability of staff both internally and externally when having to maintain service with paper and manual processes.

Experiencing a similar experience at her facility, Sara Harm, MD, MSc, from the University of Vermont Medical Center, described a phishing cyberattack in 2020 that impacted the hospital's system for 25 days, resulting in a $46 million loss in incremental recovery cost, which was only partially covered by insurance. By continuously adapting to manual processes and reverting to "old school" technology like jump drives, fax stamps and lab runners, there were no breaches of patient or employee data and no adverse patient

Helpful Cyber Resources from 2024 AABB Cybersecurity Executive Summit:

ORGANIZATION/SUBJECT	CONTACT INFORMATION
HHS Office of the Assistant Secretary for Preparedness and Response (ASPR)	https://aspr.hhs.gov/Pages/Home.aspx
HHS Cybersecurity Performance Goals (CPGs)	https://hhscyber.hhs.gov/documents/cybersecurity-performance-goals.pdf
HHS HPH Cybersecurity Gateway	https://HPHcyber.hhs.gov Email: HHScyber@hhs.gov
Health-ISAC	https://health-isac.org/ https://health-isac.org/community-services/ Email for technical info: toc@h-isac.org Email for membership: contact@h-isac.org
CISA Incident Reporting System If there is a suspected or confirmed cyberattack affecting core government or critical infrastructure functions	https://myservices.cisa.gov/irf CISA Central 24/7 watch Email: report@cisa.gov or central@cisa.dhs.gov Phone: (888) 282-0870
Anti-Phishing Working Group (APWG) To report phishing scams	Email: phishing-report@us-cert.gov
FDA OBRR general inquiries	Email: cberobrrbpbinquiries@fda.hhs.gov https://www.fda.gov
FDA CBER guidance agenda, updated semi-annually	https://www.fda.gov/vaccines-blood-biologics/biologics-guidances/blood-guidances
FBI Cyber Respond and Report To report an ongoing cybercrime, threat to life or national security threat, file a report online or contact your local FBI field office	https://www.fbi.gov/investigate/cyber#Respond-and%20Report https://tips.fbi.gov/home https://www.fbi.gov/contact-us/field-offices

> "It is critical that disaster planning includes contingencies focused on cyber preparedness and the resilience of organizations within the blood supply chain."

events. Lessons Vermont Medical Center learned included the importance of segregation of internal networks, maintaining a list of system dependencies continuously, being able to increase people resources in an emergency and encouraging an environment that clearly defines priority of keeping operations running by embracing action and not punishing mistakes during the disaster.

Wrapping up the second panel, Martin Grable, executive vice president and chief financial and administrative officer of OneBlood in the Southeast, described the recent experience of a ransomware attack on his blood center. He reiterated the theme of having a preparedness plan and practicing or exercising that plan repeatedly to ensure a calm recovery process and institutional resilience. Because his center was organized, the staff was able to quickly contact authorities, including the FBI and U.S. Food and Drug Administration (FDA), as well the "breach team" with internal staff, law experts specialized in cyber events, cyber forensic experts and network recovery specialists.

OneBlood worked with the AABB Disaster Task Force and Florida Hospital Association to communicate important updates about the blood supply so that other regional and national blood providers could assist with recovery efforts. They also utilized "old school" technology in their recovery processes with jump drives, laptops and printers off-network and hotspot usage for connectivity, similar to what was used at the University of Vermont Medical Center.

Key Highlight: Cybersecurity Challenges and Opportunities Related to the Blood Supply Chain

Finally, the third panel of the summit focused on challenges and opportunities related to the blood supply chain, as the blood supply chain is a lifeline that must remain secure and resilient in times of disaster as all the previous speakers emphasized. Vikas Mahajan, vice president of information security at the American Red Cross, stated that "a cyber incident is a business problem, not just an IT problem." This statement was supported by the other participants in the third panel: Bill Block, president and CEO of Blood Centers of America; and Ann Eder, MD, PhD, director of the Office of Blood Research & Review at the FDA.

Because cyberattacks are computer-related, the tendency is to focus on information technology. However, businesses cannot afford to not be prepared or resilient because the mission of a business is dependent upon understanding and safeguarding many of an institution's business-critical systems and workflows. Block reminded us that we needed to pay special attention to the resiliency of sole suppliers in our field, such as blood bags, that could have a profound impact on the entire supply chain if targeted.

Finally, Eder reiterated that cybersecurity attacks threaten the safety of the blood supply, making it an issue for FDA as it impacts patient care. She reviewed the role of the FDA in cyber through regulation of device manufacturers and blood establishments and mentioned a potential upcoming draft guidance on reporting to FDA in case of cyber events. The third panel emphasized the importance of health care organizations using the DHHS CPGs for cyber preparedness and resiliency.

In conclusion, to ensure we are all prepared for WHEN the next cyberattacks occur, it is critical that disaster planning includes contingencies focused on cyber preparedness and the resilience of organizations within the blood supply chain. For further education and contact information, please refer to the summary list of resources provided by the speakers of the AABB Executive Cybersecurity Summit or reach out to the AABB Information Systems Committee for additional information. ■

Scan the QR code to watch the recording of the Summit