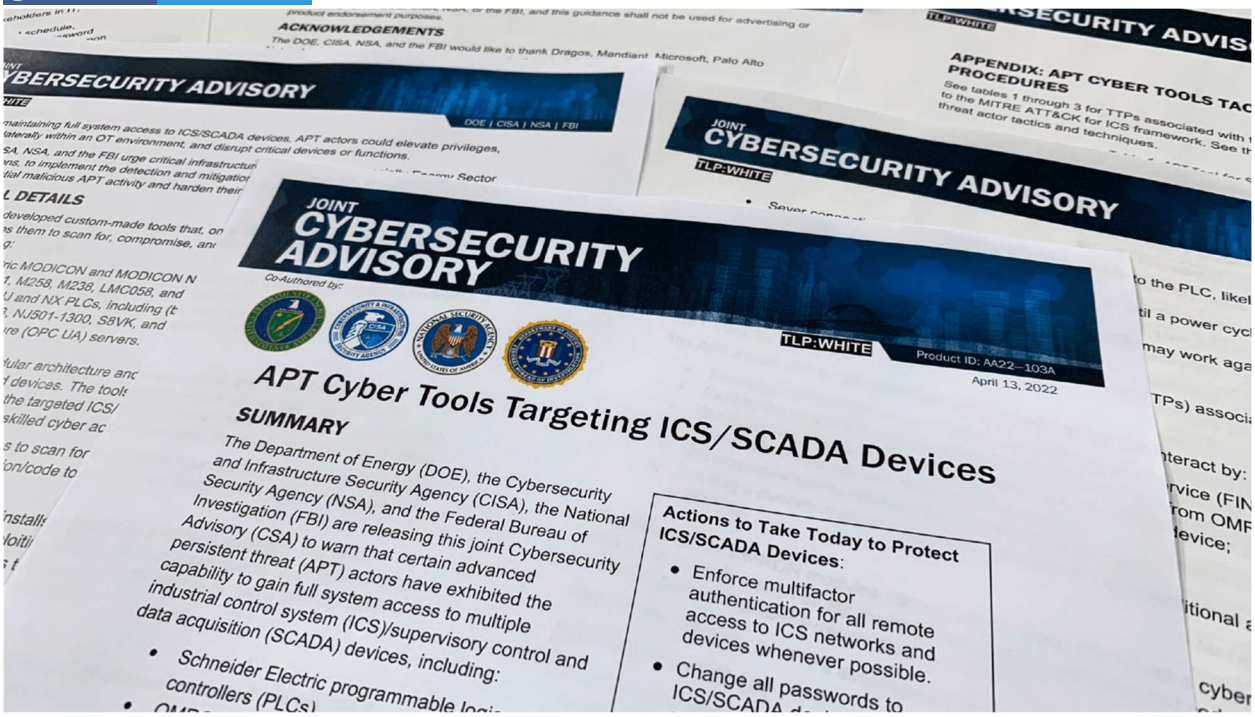
OPINION>CYBERSECURITY

THE VIEWS EXPRESSED BY CONTRIBUTORS ARE THEIR OWN AND NOT THE VIEW OF THE HILL

How corporate boards can ensure cybersecurity is mission critical

BY SANJAI BHAGAT, OPINION CONTRIBUTOR - 12/27/22 4:00 PM ET

SHARETWEET



(AP Photo/Jon Elswick)

A joint cybersecurity advisory released by the Department of Energy, the Cybersecurity and Infrastructure Security Agency, the National Security Agency and the FBI is photographed in Washington, Wednesday, April 13, 2022. The agencies issued the joint alert Wednesday announcing the discovery of malicious

cyber tools capable of gaining "full system access" to multiple industrial control systems. (AP Photo/Jon Elswick)
Cybercrime is a threat to our nation, including our health care systems, financial systems, public utilities and national defense infrastructure.

Global cybercrime costs between $6 and $7 trillion annually. To understand the size of this loss, the annual GDP of the top three countries in the world is the U.S. with $20.4 trillion, China with $13.4 trillion and Japan with $5 trillion. For another perspective on the size of cybercrime losses, Home Depot, Target and Sony shareholders lost 5 to 10 percent of their market capitalization when the stock market learned of their cybercrime data breaches.

How should corporate board directors think about cybersecurity governance?

The Caremark International Inc. Derivative Litigation ruling is a decision issued by the Delaware Chancery Court in 1996 that provides the legal framework for a corporate board of directors' responsibilities regarding cybersecurity governance. The original Caremark decision was not about cybersecurity governance; Caremark placed a requirement on directors that they establish an information and reporting system in the company that would be designed to deter, detect and inform them of corporate negligence. It also required ongoing oversight of this system by the board and the board's response to red flags.

For about two decades after the Caremark decision, it was not on the corporate governance radar until the Delaware Supreme Court reversed the ruling of the Delaware Chancery Court in 2019 in Marchand v. Barnhill. Marchand involved a Caremark

claim against Blue Bell Creameries USA after some of its customers died after consuming listeria-infected ice cream. The Delaware Chancery Court dismissed the claim by noting that Blue Bell had a compliance program to ensure food safety. The Delaware Supreme Court reversed the Chancery court's decision; the basis for their decision was (a) food safety was *mission critical* to Blue Bell, and (b) the company's directors did not establish a process to get *regular* reports from management on food safety and violations of food safety.

After the Delaware Supreme court's decision on Marchand, the Delaware Chancery Court has applied an *enhanced* Caremark standard to several cases during the past three years. The Chancery Court is focusing on whether the litigation issue involves a *mission critical* aspect of the company, and whether the board had established procedures to get *regular* reports from management on the mission critical aspect of the company.

Given the enhanced Caremark standard, and that cybersecurity is mission critical for most companies, I suggest the following cybersecurity governance principles:

First, a company must have procedures in place to detect cybersecurity threats and incidents and report them to management in real time. The plan should include a protocol to respond to a breach in customer data, including who should be contacted and when as well as the process for reporting this to the public. Management and board members should review the storing and accessing of customer data.

Second, management must report cybersecurity threats and incidents to the board on a timely basis.

Third, boards must discuss cybersecurity on a regular basis, not just after a cybersecurity incident.

Fourth, IT cybersecurity experts need to focus on potential cyberattacks that can cause the most *economic* harm to the company. IT cybersecurity experts tend to be focused on defending any and all cyberattacks, and incorporating a (mostly software-based) fix of actual and potential attacks, whereas corporate directors are focused on the impact of cyberattacks on the company's long-term shareholder value. This suggests that resilience to cyberattacks is as important as defense from cyberattacks.

Southwest Airlines meltdown: When ultra-efficiency is not supported by technologyRanked choice voting solves politics' 'spoiler problem'

Finally, while a board sub-committee on cybersecurity is not essential, a board sub-committee should be designated whose main responsibility is cybersecurity. This cannot be the audit committee, given the different skill sets needed for audit and cybersecurity governance.

Corporate boards that focus on these cybersecurity governance reforms will be better able to serve their stakeholders today and in the future.

Sanjai Bhagat serves on corporate boards, is a professor of finance at the University of Colorado at Boulder and author of "Financial Crisis, Corporate Governance, and Bank Capital" (Cambridge University Press).