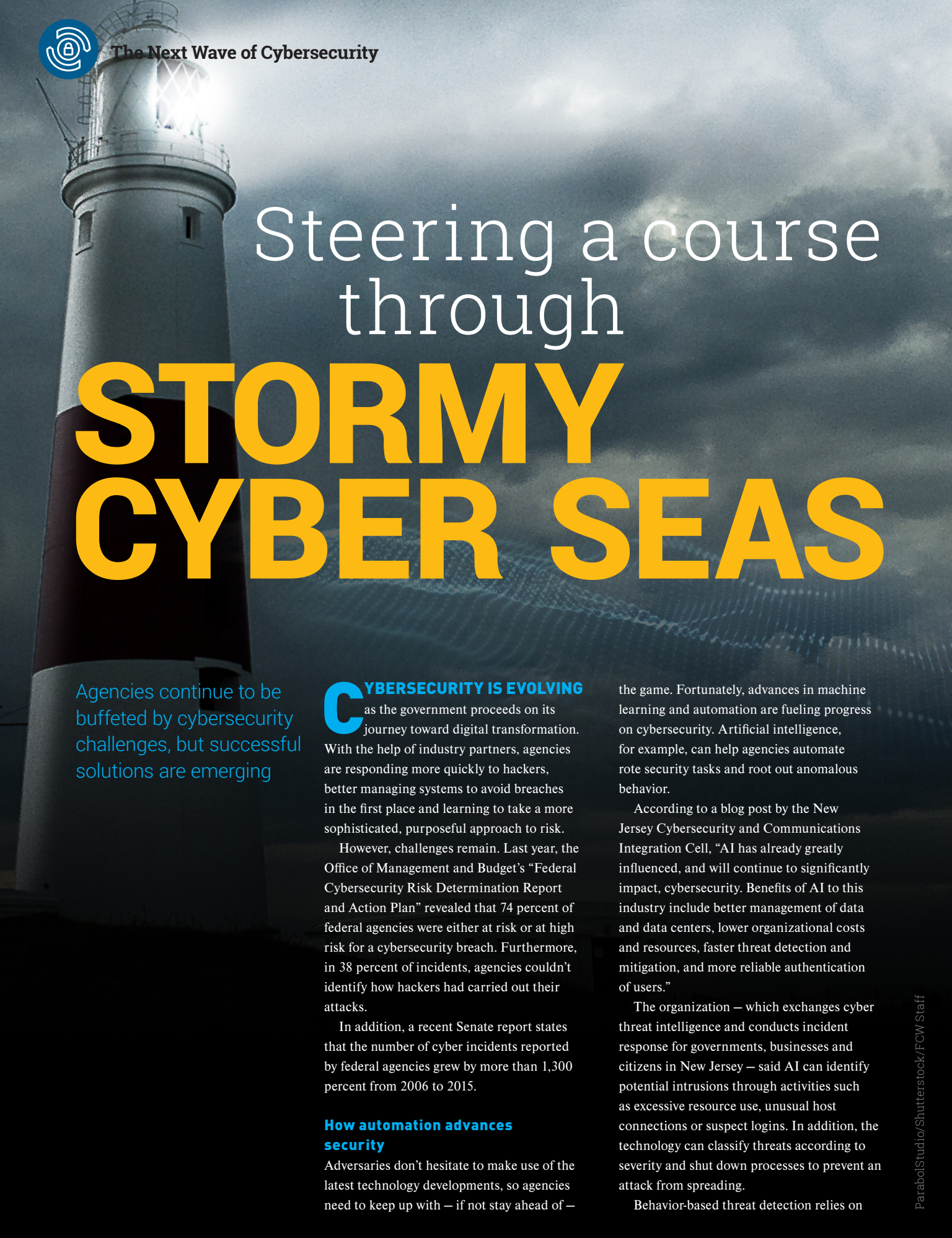

Steering a course through STORMY CYBER SEAS

Agencies continue to be buffeted by cybersecurity challenges, but successful solutions are emerging

CYBERSECURITY IS EVOLVING as the government proceeds on its journey toward digital transformation. With the help of industry partners, agencies are responding more quickly to hackers, better managing systems to avoid breaches in the first place and learning to take a more sophisticated, purposeful approach to risk.

However, challenges remain. Last year, the Office of Management and Budget's "Federal Cybersecurity Risk Determination Report and Action Plan" revealed that 74 percent of federal agencies were either at risk or at high risk for a cybersecurity breach. Furthermore, in 38 percent of incidents, agencies couldn't identify how hackers had carried out their attacks.

In addition, a recent Senate report states that the number of cyber incidents reported by federal agencies grew by more than 1,300 percent from 2006 to 2015.

How automation advances security

Adversaries don't hesitate to make use of the latest technology developments, so agencies need to keep up with — if not stay ahead of — the game. Fortunately, advances in machine learning and automation are fueling progress on cybersecurity. Artificial intelligence, for example, can help agencies automate rote security tasks and root out anomalous behavior.

According to a blog post by the New Jersey Cybersecurity and Communications Integration Cell, "AI has already greatly influenced, and will continue to significantly impact, cybersecurity. Benefits of AI to this industry include better management of data and data centers, lower organizational costs and resources, faster threat detection and mitigation, and more reliable authentication of users."

The organization — which exchanges cyber threat intelligence and conducts incident response for governments, businesses and citizens in New Jersey — said AI can identify potential intrusions through activities such as excessive resource use, unusual host connections or suspect logins. In addition, the technology can classify threats according to severity and shut down processes to prevent an attack from spreading.

Behavior-based threat detection relies on

ParabolStudio/Shutterstock/FCW Staff

AI's ability to monitor user characteristics such as gait, keystrokes or work habits so that administrators can be alerted as soon as something out of the ordinary happens, which could signal a breach.

Advances in automation also help agencies make sense of threat intelligence and free the security team to focus its efforts on solving more complex cybersecurity challenges. However, many Americans are wary about the use of AI and its implications for privacy.

In a survey conducted by the Center for the Governance of AI, researchers wrote that "Americans express mixed support for the development of AI. After reading a short explanation, a substantial minority (41 percent) somewhat support or strongly support the development of AI, while a smaller minority (22 percent) somewhat or strongly opposes it."

Agencies are taking action to address those concerns in concert with private-sector experts and members of the public. For instance, the National Science Foundation is partnering with Amazon on the Program on Fairness in AI "with the goal of contributing to trustworthy AI systems that are readily accepted and deployed to tackle grand challenges facing society."

And the National Institute of Standards and Technology is asking federal agencies, the private sector and academia to weigh in on efforts to formulate technical standards for AI.

Building a more secure workforce

Despite changes in the cybersecurity landscape, users remain a key point of vulnerability. Experts cite the proliferation of unapproved devices connecting to agency networks and the increasing sophistication of phishing attempts as vectors for attack — not to mention the boom in internet-of-things devices that lack built-in security features.

"Hackers are able to get past military-grade firewalls since they no longer have to battle their way through the network," according to an article published in Forbes earlier this year. "Instead, they find it much easier to detect a poorly protected or managed endpoint device."

Therefore, it is essential that agencies have comprehensive visibility into their networks (whether on-premises or in the cloud) so that they can manage the performance and security of an increasingly complex IT environment. Zero-trust strategies are one way that agencies can protect resources by limiting user privileges. The goal is to safeguard high-value assets while supporting employee productivity and collaboration, especially as the government workforce becomes more mobile.

The draft Federal Data Strategy recognizes the important role that employees must play in security, and it highlights the need to develop appropriate skills across the federal workforce. "Data-driven decision-making requires not only accessible, high-quality data but also a workforce with adequate knowledge of data security practices and data skills... to leverage insights from data while also safeguarding protected information," according to the action plan for the strategy.

Balancing the need for access with the need for security is an ongoing challenge, and government agencies must continue to use every tool at their disposal. ■

EMERGING CYBERSECURITY TRENDS by the numbers

88%
Public-sector organizations that have experienced at least one cyberattack in the past two years

33%
IT security practitioners who said their organizations are effective in reducing the risk from unapproved apps and devices

64%
Organizations that experienced successful attacks launched at their endpoints in 2018

$17.4B
Proposed cybersecurity spending in the Trump administration's fiscal 2020 budget request

82%
Survey respondents who believe robots and/or AI should be carefully managed

Sources: Center for the Governance of AI, Ponemon Institute, Tenable, White House