Corporate Cybersecurity Expert Says Think Like an Attacker to Improve Information Security

“You’ve got to be able to take a punch in this environment,” said Lt. Gen. Matthew Glavy, the Marine Corps Deputy Commandant for Information. *LISA NIPP*

NATIONAL HARBOR, Md. — The U.S. government, military and private sector need to change the way they perceive cybersecurity and look at it from the attacker’s point of view, the global head of IBM’s X-Force said.

“I think that we will look back at 2022 as a tipping point for information security and the way we work with each other: private sector, public sector. Really, all of these silos which we’ve built up are meaningless for attackers,” Charles Henderson said April 5 during a panel discussion on maritime cybersecurity at Sea-Air-Space 2022.

“They care about their rules, not yours,” he continued. “All too often in information security, whether it’s public sector, private sector or somewhere in between, we tend to think of our own goals and not the goals of the attacker. I think if we’re going to be successful, we need to turn that on its head and start looking at everything through the eyes of an attacker.”

All of the panelists agreed that keeping information secure is essential to maintaining an advantage over adversaries and keeping them from gaining an advantage.

Navy Rear Adm. John Okon, the head of the Warfare Integration Directorate (N2/N6F) in the Office of the Chief of Naval

Operations, said “Cybersecurity is really about warfighting. It’s important that we get cybersecurity right, up front, if we’re going to be a lethal, agile and ready force.” To underscore its importance, Okon called cybersecurity “commanders’ business,” but he added that “everyone that puts their fingers on a keyboard has a role in responsibility and accountability for cybersecurity.”

Okon said the Navy Department needed to shift its culture from compliance to readiness. “Expect what you inspect. That’s walking the deck plates every day, looking at your network every day.” Making sure that the speed from when a vulnerability is identified to a patch is in place comes not in weeks, “but minutes or seconds.”

Lt. Gen. Matthew Glavy, the Marine Corps Deputy Commandant for Information, said the side that is able to maintain the information advantage “has an edge.” That edge could be system overmatch, a good prevailing narrative of “trusted, competent, delivered with trade craft,” or resiliency. “You’ve got to be able to take a punch in this environment,” Glavy said “and the side that can take that punch and either counterpunch or begin anew, creates an edge.”

The Marines are in the final stage of crafting a new information doctrine, Marine Corps Doctrinal Publication 8 Information “all founded on our warfighting construct of maneuver warfare.”

“Protecting your own backyard, you’ve got to have a good defensive perimeter and terrain that you can defend to ensure your capabilities are available where and when you need them. That’s job one for us,” said Rear Adm. Mike Ryan, commander of Coast Guard Cyber. He said the Coast Guard was following the lead of U.S. Cyber Command, generating forces that allow the agency to provide the entire spectrum of capabilities to protect the homeland, ensure mariner safety and secure the $5.4 trillion economic activity that arrives on U.S. shores by

maritime commerce.