Our Collective Response to SolarWinds Cyber Attack

William J. Bender
Chief Information Officer, US Air Force (retired)
Senior Vice President
Leidos

When I first learned of the damaging SolarWinds attack on U.S. Government agencies and contractors, I thought about how I might have responded to the incident if it had happened on my watch as USAF Chief Information Officer (CIO). Almost immediately, senior IT leaders recognized the potential long-term ramifications to national security. While recognizing a problem is important, how you react and what steps you take to address the problem is what matters. Harkening to my experience as an Air Force pilot with over 4,000 flight hours, I couldn't help but think the procedures taught in pilot training on ground and inflight emergencies would apply equally well in our collective response to SolarWinds. In priority order: maintain controlled flight, analyze the situation and decide on proper actions, complete applicable emergency procedures (those committed to memory) and, finally, refer to the flight manual and complete remaining actions.

> "Harkening to my experience as an Air Force pilot with over 4,000 flight hours, I couldn't help but think the procedures taught in pilot training on ground and inflight emergencies would apply equally well in our collective response to SolarWinds."

Assess The Situation

The SolarWinds equivalent of maintaining controlled flight is to assess the situation at hand in order to understand the problem as much as possible with the information available. In this case, it is important to know SolarWinds as a prominent supplier of network and server management tools used to instrument, monitor and provision IT devices, deployed extensively within the US Government and by a majority of the Fortune 500. Equally important is to assess whether the incident is really a problem and not just an anomaly or a nuisance. Over the years, professional pilots and aviation enthusiasts alike have heard too many stories of flying perfectly good aircraft into the ground because a burnt out light bulb mistaken for an inflight emergency. The same is true for cyber incidents.

Analyze The Situation

Analyzing the situation requires that you move past immediate recovery actions to a well-thought response plan. SolarWinds, for example, was a very sophisticated nation-state attack whereby malware was in the software development life cycle and distributed to customers during regular updates. Adding further complexity, the software continued to function normally even after the malware activated to allow privileged access to the attacker and the ability to move laterally between servers. Whereas returning to controlled flight is dependent on "what" happened, deeper analysis seeks to determine "where" you might be exposed and "how" the malware could negatively affect operations. Because SolarWinds was not a software vulnerability per se, resolving the issue requires more than a simple patch. Instead, the malware was part of the base build and would need

Continued on page 28

Lt. General William J. Bender (retired) most recently served as CIO for the Air Force, where he was responsible for 50,000 cyber operations and support personnel across the globe with oversight for the USAF's IT investment strategy and a portfolio valued at $17 billion. After retiring from the Air Force following a 34-year career there, Lt. General Bender joined Leidos in September 2017. Now tasked with overseeing and managing the Strategic Account Executives, a group of customer-facing senior-level former government officials, Lt. General Bender aims to bolster customer relationships and advance strategic initiatives to foster organic growth.

to be removed and replaced with a clean version.

Responding To Incidents

Responding to a cybersecurity incident, similar to an aircraft emergency, is time sensitive. In some cases, time does not allow long deliberation and consultation before taking action. Immediately upon identifying the SolarWinds breach, CISA published a directive to all government agencies running the software to shut down all instances, to perform forensics and to report any compromises. Industry was asked to consider taking the same actions. Follow on actions might allow time for more discussion and a more deliberate approach. After completing all emergency actions to put out an engine fire from memory, pilots refer to the flight manual to read procedures and complete the actions necessary to prepare for an engine out landing. Loading indicators of compromise onto network sensors to detect and prevent the malware from beaconing out to the Internet is one such action. Another would be to complete more thorough discovery of other instances on other agency or company networks and servers, and to assess risk and direct specific actions. Finally, sharing information and coordinating with the likes of CISA and the DIB, while not an immediate action, is important all the same.

The CIO’s Crucial Role

CIO organizations across government and industry have transformed in recent years from that of procuring and maintaining IT, to having a central role in the development of networks, IT systems and data bases in support of enhanced operations. In that way, CIO priorities and activities, like the networks and data they manage, tie inextricably to operational success. CIOs now have a seat at the table and their collective response to the SolarWinds breach in the days and months ahead will go a long way to ensuring they remain there. ■