5 LESSONS from 2020's Defining CYBER ATTACK

By Brunswick Senior Advisor **MIKE ROGERS,** former Commander of the US Cyber Command.

IT HAS BEEN MORE THAN THREE MONTHS since the cyber attack on SolarWinds was first reported, a business whose 320,000-plus clients include the US departments of Treasury, Justice, and Commerce, as well as 499 of the companies on the Fortune 500.

And yet it's still too soon to say what the long-term effects of that attack will be: The acting director of the US Cybersecurity and Infrastructure Agency said in early March that understanding the full extent of the

ILLUSTRATION: DAVID PLUNKERT

damage would take months—while fully securing compromised government networks could take as long as a year and a half. ■ Still, some lessons have already emerged. Popular perceptions aside, this wasn't the work of a young hacker working out of a basement. We have seen yet again the lengths that focused, determined adversaries are willing to go to in order to launch long-term supply-chain attacks—one tech executive estimated the SolarWinds attack to be the work of "1,000 very skilled, very capable engineers." As businesses consider their own cyber resiliency against such sophisticated, evolving threats, they should bear the following lessons in mind:

1 **Don't succumb to a false sense of security—everyone's at risk.** Businesses now rely on an ecosystem of suppliers and third-party vendors for services and software—and each provide a possible entryway for threat actors. The SolarWinds attack involved inserting malicious code into one of SolarWinds' systems—code that went undetected for as long as nine months and which, when SolarWinds sent out a software update, spread to potentially tens of thousands of users.

Supply-chain attacks are inherently indiscriminate: when a threat actor is able to access an ecosystem of networks, they can access data from everyone, not just the initial target. An organization's size, sector, and function provide no immunity—threat actors do not recognize borders, nor do they care about the sectors or the silos within an organization. Every business is built around network access both internally and externally. With SolarWinds, we saw the adversary turn the network against itself.

2 **Be proactive.** A natural response to SolarWinds is to focus on mitigating supply-chain attacks. But threat actors are actively seeking and exploiting any vulnerabilities they can find, including in non-supply-chain-related hardware and network protocols. Don't limit your response or planning. Be proactive, evolve your thinking and approach—that's what threat actors are doing.

3 **A strong cyber strategy focuses on defense and resilience.** Organizations often think they need only consider how to prevent cyber breaches. Yet large-scale breaches like SolarWinds reinforce that the ability to operate in the face of a cyber crisis is equally important. Invest in both cyber resiliency and defense equally.

4 **Know your supply chain.** This sounds basic, but it's fundamental: build a deep knowledge of the companies whose products and services you rely upon and use. This strong working knowledge of your own supply chain forms a crucial, integrated part of assessing your cyber maturity and resiliency.

5 **Create accountability, not silos.** A lack of personal and organizational accountability for protecting sensitive data and infrastructure can compound a cyber attack. Rather than be treated as a secondary or tertiary function, cybersecurity should be integrated across the entire company—because it affects the entire company. The fear, loss of trust, and reputational damage in the aftermath of a cyber attack often linger after the attack is "over" and your network is secure. This gets to the heart of the matter: understand cybersecurity isn't a technology concern, but a critical business issue. ◆

UNDERSTAND CYBERSECURITY ISN'T A TECHNOLOGY CONCERN, BUT A CRITICAL BUSINESS ISSUE.

In a 37-year career with the US Navy, **MIKE ROGERS** rose to the rank of four-star admiral, ultimately serving as Commander of the US Cyber Command, leading teams that stopped the most destructive cybercriminals in the world. He served as Director of the National Security Agency, the largest US intelligence agency, and as Chief of the Central Security Service. He is now a Brunswick Senior Advisor in Brunswick's Washington, DC office.

Additional reporting by **ELIZABETH NORTON,** an Executive in Brunswick's Cyber Practice, who is also based in Washington, DC.