From the Desk of
***Lieutenant General Lori Reynolds**, USMC (Ret.)*

Log4j for Leaders

For many non-technical business leaders, news of cyber vulnerabilities are opportunities to be silently grateful for smart cybersecurity teammates and CISOs. In most cases, once vulnerabilities are identified, IT teams scan systems for evidence of the vulnerabilities, prioritize mitigation efforts and then patch as soon as patches are available. CISOs report compliance, and everyone moves on. The Log4j vulnerability will be different, and leaders should pay attention.

Log4j is found in a free, open-source JAVA logging tool that's widely used globally in software, networks (servers and virtual machines), operational technology, games, mobile devices and any other device that can be found on the Internet of Things (IOT.) Many businesses are under attack now from exposure to this vulnerability. There will be few businesses or IT teams who escape this one, because the problem is prolific. And in this instance, cyber attackers absolutely have the advantage, because Log4j is ubiquitous and its vulnerabilities are easy to exploit. Moreover, even if you properly secure your own environment from Log4j exposure, you could be vulnerable to third-party or partner applications or technology using the Log4j tool.

There is a great deal of reading available on the internet for leaders and cybersecurity professionals on the Log4j vulnerability and how to scope the problem, mitigate its effects and recover security. That's not the central message of this note. As 2021 comes to a close, this vulnerability presents a great opportunity for CEOs and leadership teams to ensure that you are properly organized for the cyber environment we find ourselves in. Log4j is a wake-up call – the cyber threat is real, demands leaders' personal attention and isn't just work for IT techs to be concerned about. Log4j is a reminder that our workplaces rely on secure cyber environments, trusted partners who value security as much as we do, and employees who can be trusted to properly operate in a contested cyber environment. And given attackers' race to exploit this vulnerability, Log4j is a reminder that bad actors are abundant and eager to exploit vulnerabilities like Log4j.

(continued on page 2)

(cont.)

Here are my recommendations:

1. Take good care of your cybersecurity team. This vulnerability, in particular, is really difficult to mitigate and isn't going away soon. Stay interested in what your team is doing and how you can help them succeed. Be professionally curious about threats to your operating environment and give your IT teams tools to be successful.

2. If you don't already have "tech to leader" discussions on the schedule, think about making that part of your battle rhythm for 2022. Log4j won't go away anytime soon. In fact, Log4j exposed your business to attackers and opportunists already. Even if your team has properly scoped and managed the risk to your infrastructure, you are also dependent on third-party applications and interfaces that are also vulnerable. Your guidance to your tech team on what cyber terrain matters to you is important. Consider wargames or readiness drills with your executive team to help you think through response options if/when you are attacked.

3. Make cybersecurity part of your business culture. It's not enough to conduct annual training with a compliance mindset. Your cyber environment exposes you to insider threats, external attacks and opportunists. Every employee has to play a role in defending your business. Actively defending across your team is more effective than relying on the IT team to recover security once an attack happens.

4. Seek alliances outside your business. We all rely on other businesses and supply chains to be successful. How vulnerable are you to business partner cybersecurity practices and infrastructure? Adopting a teamwork mentality in cyber can help reduce surprise, strengthen partnerships and fight back against determined or opportunistic attackers. Cybersecurity is a team sport.

As we all learned during the Colonial Pipeline attack, cyber attacks can have consequences we haven't fully imagined. In the spirit of "Never let a good crisis go to waste," consider using the Log4j crisis as an opportunity to ensure that your leadership team and employees are prepared for a very active cyber threat environment in 2022.