Armstrong Teasdale

December 28, 2021 • Advisory • www.atllp.com

LOG4J HIGHLIGHTS LEGAL OBLIGATIONS FOR BUSINESS LEADERS

Two weeks ago, we briefly discussed the potential legal implications for failing to respond to cyberattacks on supply chain technologies. At that time, Log4j, the critical vulnerability that was discovered in an application used in many software products, had been publicly disclosed for a few days.

The fallout since has been intense. Just as the destructiveness of the Log4j vulnerability has been well publicized – achieving "a severity score of 10 out of 10" by one cybersecurity analyst – so too has advice on how to respond. Task forces have been formed, vulnerability scanners have been released, and agencies have issued detailed guidance.

As to cybersecurity readiness, Log4j is just the latest of many incidents highlighting the importance of supply chain risk management and related legal obligations. Recent lawsuits against SolarWinds, Colonial Pipeline and ParkMobile have asserted that failing to patch vulnerabilities is evidence of negligence.

In each of the above cases, the plaintiffs cited the Federal Trade Commission. In April the FTC issued detailed guidance on the role business leaders must play in cybersecurity, stating "[c]ontrary to popular belief, data security begins with the Board of Directors, not the IT Department."

Based on our involvement in hundreds of cybersecurity incidents, we have observed that business leaders and IT teams that work closely together give their organizations the best chance of avoiding litigation and regulatory investigations. In many of these situations, we collaborate with technical consultants just as business leaders do with their IT teams.

Technical consultant Digital Silence, for example, is monitoring the Log4j vulnerability closely. It recommends that organizations focus on ensuring their security systems are configured to protect against it by:

- Ensuring that the security tools used within your organization have been patched and are running the latest revision from the vendor. You can find an active list of products and services and their current status at Tech Solvency.
- Utilizing your vulnerability management and asset management processes to identify vulnerable hosts, endpoints and cloud services that may need updates. Leverage your emergency patching procedures

PEOPLE

Jeffrey Schultz, CIPP/US

SERVICES AND INDUSTRIES

Data Innovation, Security and Privacy

as the CVSS Score for both (CVE-2021-44228 and CVE-2021-45046) Log4j vulnerabilities is the highest at 10, which signals that immediate patching is required.

- For organizations with internet-facing applications, ensuring that their Web Application Firewalls (WAFs) have been configured to detect and deny any potential Log4j attacks.
- Validating that endpoint protection solutions such as Endpoint Detection and Response (EDR) and Managed EDR (MDR) are monitoring for Log4j attacks.
- Leveraging your established incident response plans. While this vulnerability is critical and widespread, using your established policies and procedures can ensure a successful response to this crisis.

The above recommendations are separate from the legal recommendations we previously provided. We encourage business leaders and IT teams to continue to monitor trusted news outlets for technical information, including CISA and the SANS Internet Storm Center. We also encourage organizations that share personal information with service providers (or other vendors) to reach out to them to assess whether their service providers are likewise diligently responding to the risks associated with Log4j.

Given the litigation and regulatory investigations that have occurred this year, organizations that experience cybersecurity incidents as a result of the Log4j vulnerability may also find themselves having to defend against allegations of negligence. Following this guidance could enable organizations to be prepared for, and possibly preempt, such allegations.