We are aware of the worldwide proliferation of internet-based attacks and their potential impact on cybersecurity and data protection. We have observed that internet-based attacks have increased across many geographical regions which are commonly associated with cybercrime. Our end-to-end control processes constantly evaluate vectors for attack origination. In order to harden and secure all of our systems that store or transmit electronic information, we have implemented multi-layered preventive controls across our perimeters, technology infrastructure and end-point computing. Additionally, we have implemented advanced threat technologies, such as web and cloud application firewalls, which use aggregated intelligence to proactively detect and block an overwhelming majority of attacks. Lithia Motors has significantly expanded its footprint of information security solutions to monitor internet-based attack vectors as well.

We identify vulnerabilities in our information systems through proactive scanning of system assets for known vulnerabilities published by the National Institute of Standards and Technology (NIST). Our outsourced managed security source operates 24/7, identifying vulnerabilities. Additionally, we proactively manage vulnerabilities from major software publishers through a global patching program. We continue to monitor and enhance our internal processes and intend to conduct a self-audit.

In order to prevent unauthorized access to our information systems, we have a system of controls in place to manage user access under auditing from a third party and as part of management's Sarbanes-Oxley (SOX) controls. Our employees sign an acceptable use policy and are trained on how to identify information security risks in the workplace and in their personal lives.

Our information security policy is aligned with the National Institute of Standards and Technology (NIST) and the Center for Internet Security (CIS) as it relates to procedures, processes, training and awareness and critical technology controls.