FEDERAL SIGNAL
Moves. Cleans. Protects.

1415 West 22nd Street, Suite 1100
Oak Brook, Illinois 60523
630.954.2000
federalsignal.com

Company response to cyber-security risks

The Company has observed a global increase in information technology ("IT") security threats and more sophisticated cyber-attacks. The Company's business could be impacted by such disruptions, which in turn could pose a risk to the security of the Company's systems and networks and the confidentiality, accessibility and integrity of information stored and transmitted on those systems and networks. The Company has adopted measures to address cyber-attacks and mitigate potential risks to the Company's systems from these information technology-related disruptions.

Matters relating to the Company's IT initiatives and risk management process are discussed at the Company's IT council meetings, which are held quarterly. Members of the Company's IT council include the Company's Chief Executive Officer, Chief Operating Officer, Chief Financial Officer ("CFO"), Chief Compliance Officer, Chief Information Officer, Corporate Controller, Director of Internal Audit, Chief Information Security Officer, and several business unit/group management representatives.

The Chief Information Officer presents any significant IT matters to the Board of Directors. Such presentations are held at least annually, and more frequently if considered necessary. The most recent update was presented to the Board of Directors in December 2022, when the Company presented an update on the progress that it has made against several cyber-security initiatives. Of the Company's seven current directors, six are considered independent, and several have had prior responsibilities overseeing IT functions at various organizations.

The Company's management is responsible for establishing and maintaining an adequate system of internal control over financial reporting, which includes controls over the Company's key IT systems. As part of its annual assessment, controls around IT system access, program change, and security are evaluated for effectiveness. Based on the most recent assessment completed, both management and the Company's Independent Registered Public Accounting Firm concluded that, as of December 31, 2022, the Company's internal controls over financial reporting were effective.

The Company's management places reliance on the work of its Internal Audit department in making its assessment of the effectiveness of internal controls. To provide for the independence of the Company's Internal Audit department, its personnel shall report to the Company's Director of Internal Audit, who shall report functionally to the Company's Audit Committee and administratively to the CFO.

The Company's Audit Committee currently comprises three, independent directors, each of whom are financial experts. Among the responsibilities listed in its Charter[1], the Company's Audit Committee is

[1] https://6860826.fs1.hubspotusercontent-na1.net/hubfs/6860826/Federal%20Signal/Governance/Audit%20Committee%20Charter.pdf

responsible for reviewing and discussing with management and the independent auditor the adequacy of the Company's internal controls, including information technology, cybersecurity and financial reporting controls.

As part of the Company's cyber-security risk management process, the Company has implemented a variety of tools to assist employees in identifying potential threats and educating employees on information security best practices. The Company has an information security training and compliance program and has also invested in software designed to identify potential threats.

The Company also engages third-party consultants with information security certifications to perform external penetration tests, taking actions to address any recommended improvements, where applicable.

The Company has entered into an information security risk insurance policy with a reputable insurance provider.

In the last three years, the Company has not experienced any significant information security breaches, and net expenses from information security breaches, breach penalties, and settlements were insignificant relative to total revenue.

However, given the unpredictability of the timing, nature and scope of such disruptions, the Company's systems and networks remain potentially vulnerable to attacks. Depending on their nature and scope, such attacks could potentially lead to the compromising of confidential information, misuse of the Company's systems and networks, manipulation and destruction of data, misappropriation of assets or production stoppages and supply shortages, which in turn could adversely affect the Company's reputation, financial condition, results of operations or cash flow.