SUPPLEMENTAL DATA SECURITY DISCLOSURE AND CONSIDERATIONS

Protecting Our Assets – Data Security at SiteOne

At SiteOne, we leverage a combination of security standards and frameworks to manage and measure our cybersecurity program. As the threat actors evolve their techniques and attack vectors change, we continually update our programs for confidentiality, data integrity and availability. We have invested – and will continue to invest in – protecting, monitoring, alerting and mitigating information security risks across the enterprise.

In the event of a security issue, we have an incident response plan used to quickly triage, contain and understand the issue, as well as how to protect against it going forward. Managing our daily security program is a team of information security engineers and analysts led by our Chief Information Security Officer.

Additionally, our Privacy and Security Statement provides information regarding how we collect, use and share information we collect from our customers. We explain the ways we use the information we collect, and how customers can find out more about the personal information we collect about them on the Exercise My Privacy Rights page of our website.

Governance, Risk & Compliance

Our information security and privacy policies are in place and regularly updated based on business, compliance and any other needs.

External and internal resources perform audits and penetration testing throughout the year on SiteOne applications, networks and environments. As a publicly traded company, SiteOne is audited annually from both a financial and Sarbanes-Oxley perspective. We also engage Deloitte as our external auditor, who works with Protiviti as our staff-mitigated internal auditor. The results of these audits are presented to the SiteOne Board of Directors and any material weaknesses discovered are also disclosed to stockholders. Senior management also briefs the Board on information security matters at least annually but generally quarterly at the Board's quarterly meetings. Senior management will also discuss information security matters with the Board more frequently than quarterly, as needed.

Additionally, an external qualified security assessor performs an annual review for compliance with the Payment Card Industries Data Security Standards. SiteOne is a "Merchant Level 2" under the Payment Card Industries Data Security Standards and, therefore, has a qualified security assessor perform our PCI assessment each year. We obtain a Report of Compliance for Payment Card Industries (PCI) compliance and are audited against Sarbanes-Oxley as a publicly-traded company. We also go an extra step by obtaining a report of compliance from our qualified security assessor even though this report is not a requirement of Merchant Level 2 companies.

Data Protection

We maintain both data classification and retention policies to reduce the exposure of unauthorized access of data and comply with regulatory requirements. We strive to minimize the customer data collected to limit the potential data exposure risks.

Data is continually scanned to identify sensitive data to determine whether it is properly protected and classified. SiteOne utilizes third parties specializing in vulnerability assessments and penetration testing to review our networks, systems and applications for patching and proper configuration. We also perform at least quarterly disaster recovery test exercises annually to validate and optimize our ability to recover technology at a secondary data center site in the event of a major incident or disaster event.

Vendor Security

We partner with our vendors to minimize the customer data needed to provide services and ensure compliance with regulations. Vendors are reviewed annually to identify any changes to services, data requirements and associated security and protections. Where applicable, vendors are contractually bound to protect customer data and support enforcement of all regulatory requirements.

Data Security & Privacy Awareness

We provide new-hire and annual security awareness and privacy training to all associates; targeted security training for key departments dealing with sensitive data types; and phisher training associated with our quarterly phisher assessment program.

All new hires are required to take the training when they start with SiteOne, and all existing associates complete the training at least once annually. Our security awareness partners provide this type of training as their core business service and update their program annually to address the latest trends and risks in the information security space. Training includes SiteOne Information Security follow-up questions to ensure every associate completes the training as part of our SOX and PCI compliance.

Targeted security training includes SiteOne payment advice training to cover how to inspect payment devices for possible tampering, as well as proper credit card payment procedures. This training is required for all associates that use a payment device in their roles at SiteOne.

SiteOne also performs quarterly phishing assessment exercises to ensure associates are aware and educated about phishing threats. Any associates that click the link or attachment in the test phisher emails are assigned additional training which is tracked to completion to help them identify and avoid phishers going forward.

July 2020 Ransomware Attack

As previously disclosed, on July 14, 2020 SiteOne became aware of a ransomware attack on its information technology systems. Promptly upon its detection of the attack, SiteOne launched an investigation and notified law enforcement, and legal counsel and other incident response professionals were engaged. SiteOne implemented a series of containment and remediation measures and took steps to prevent the ransomware from spreading. SiteOne recovered all of its critical operational data, and the incident did not have a significant impact on SiteOne's business operations or ability to service its customers. At the time, SiteOne carried, and continues to carry, cyber insurance commensurate with its size and the nature of its operations. SiteOne continuously implements enhanced measures to reinforce the security of its information technology systems.

The net expenses associated with the 2020 ransomware attack included investigation expenses, professional services, legal services, technical advisory services, and cybersecurity insurance deductible and were approximately $485,000 in total, net of amounts paid by our cybersecurity insurance carrier. We also accelerated the purchase of certain hardware and software purchase that had been planned for 2021 and experienced increases in our cybersecurity insurance premiums for the years following the 2020. There were no other net expenses incurred from information security breaches over the past three years. These net expenses relative to total revenue over last three years equaled 0.006%[1]. Additionally, there were no net expenses incurred from information security breach penalties or settlements over the last three years.

[1]SiteOne's total revenue over the last three years (reported as "Net sales" in that certain Form 10-K filed on February 24, 2022) equaled $3.48 billion in fiscal 2022, $2.71 billion in fiscal 2021 and $2.36 billion in fiscal 2020.