Surmodics, Inc.
Information Technology Security Disclosure
September 30, 2022

Overview

Surmodics uses a broad array of internal resources, specialized security software, and third-party services to identify and mitigate information security risks. Our information technology (IT) security measures are designed to protect against cyber threats, detect attacks as they occur, and respond quickly and effectively to any breaches. Our cyber security program includes the following the elements:

- A data security platform designed to protect sensitive data, detect, alert, and respond to sophisticated threats such as ransomware, and help streamline privacy and compliance functions;
- A third-party threat detection and risk management services that enables us to monitor, audit and harden our environment against threats and reduce risk. This service provides 24x7 continuous monitoring and immediate alerts our IT team to suspicious activity that is detected;
- An artificial intelligence (AI) based endpoint detection and response platform designed to catch and mitigate highly advanced security threats as they emerge in real time;
- Cloud-delivered security to extend cyber protections to devices, remote users, and locations outside our facilities;
- An advanced data backup platform that offers enhanced data protection;
- Security awareness training software that allows us to educate our staff to better identify potentially dangerous content and reduce risk of a breach;
- Third-party email security with targeted threat protection;
- Enhanced firewall security;
- A dark web scanning services to detect and alert us to breached user credentials;
- Multi-factor authentication;
- Endpoint threat detection scanning and security patching tools;
- Regular external security program auditing;

- An incident response plan to address a variety of potential IT security beaches; and

- A retained third-party service to assist us in dealing with any significant IT breach, should one occur.

Our IT professionals routinely monitor and address cyber security threats as they evolve. Despite our efforts, all IT system have vulnerabilities, including user security lapses. We may not be able to protect against all threats to the security of our IT systems. Any successful cyber attack on our IT systems could have a material adverse impact on our operations, financial performance, and financial position.

IT Security Training

Surmodics conducts regular IT security training for all employees using a best-in-class third-party training platform.

External Audit of IT Security

Surmodics IT security program is audited by FRSecure who conducts an annual S2Org® Risk Assessment. The S2Org® assessment leverages and references current security frameworks and standards such as ISO/IEC 27001:2013 and the NIST Cybersecurity Framework (CSF).

IT Security Insurance

We maintain cyber security insurance designed to mitigate losses from a variety of IT security incidents. However, if we, or a third-party partner, were to fall victim to a successful cyber attack, or suffer intentional or unintentional data and security breaches by associates or third-parties, there can be no assurance that our cyber security insurance would be applicable to the specific cyber incident, that any cyber insurance proceeds would be sufficient to cover all of our losses, or that any cyber security insurance proceeds would be paid to us in a timely fashion.

Board Oversight of IT Security

Under its Charter, the Audit Committee of the Board of Director of Surmodics has the responsibility to "periodically review . . . the status of the Company's information systems hardware, software, processing procedures, including the Company's cybersecurity risks and steps that management has taken to protect against threats to the Company's information systems and security, and controls regarding accounting, internal accounting controls and auditing." 100% of the members of the Audit Committee are independent.

The company's Senior Director of Information Technology provides an annual report on cyber security to the Audit Committee. The Chair of the Audit Committee reports on each committee meeting to the full Board of Directors.

IT Security Breaches

Surmodics, Inc. has not incurred any IT security breaches that would fall within the definition of a "breach of the security of the system" as defined in Minnesota Statutes Section 325E.61 Subd. 1(e). Further, the company has incurred no IT security breach that has required notifications to be delivered to third parties under United States federal, any state law, or the laws applicable to the Republic of Ireland. Over the last three years, the company has incurred no material expenses from information security breaches, and no expenses for information security breach penalties and settlements.

The most recent IT security breach that the company's IT security systems detected prior to the date of this report was in 2019. The company can provide no assurance that there have not been undetected breaches of its IT systems.