Further Information on Information Security at OneSpan

Optimizing security efforts and limited resources to properly protect OneSpan Information Systems and Information Assets requires a structured approach to identify the various assets needing to be protected, their relative importance to OneSpan, as well as the risks faced by such assets. We identify the security measures already in place, assess their effectiveness to help measure the residual risk, and prioritize any changes that would be required to lower the risk to an acceptable level for OneSpan.

Governance

OneSpan's Information Security Risk Management Policy formalizes everyone's responsibility, from senior managers to individual users, in limiting information security risks. The policy is approved by the Information Security Steering Committee, is reviewed on a yearly basis to account for changes in OneSpan's risk environment, and describes a formal process to identify, assess and track key information security risks. Whenever required a risk treatment plan is implemented to bring risk levels below acceptable risk tolerance.

OneSpan's Information Security Steering Committee is composed of key senior leaders who operate under a formal charter. Their role is to oversee the corporate information security program and OneSpan's security posture. Their role also includes tracking progress over information security risks and approving and tracking risk-reduction initiatives. This committee conducts regular meetings, at least quarterly, with OneSpan's Chief Information Security Officer. The CISO reports to our Chief Compliance Officer (not to the Chief Information Officer) and is independent of our internal information technology group and our product groups.

The Board of Directors also oversees the progress of the information security program and the variation of information security risks through quarterly information security briefings, at a minimum. The Audit Committee has the primary responsibility for this oversight and it is comprised solely of independent directors. Our Board also includes many individuals with information security experience, such as a chief product officer at a software company, a former chief financial officer with information security oversight responsibilities, a former chief information officer who was responsible for this area, and others with various levels of experience. In total, three of the five members of the current Audit Committee have information security experience, and seven of the nine members of the Board.

Security Incidents

In the last three years we have not experienced any material information security breaches. We had a small data privacy breach in 2018 due to human error that was disclosed to the relevant data protection agency in Europe and did not result in any material expenses, no penalties and no regulatory action.

Insurance

OneSpan maintains a cybersecurity risk insurance policy and utilizes the services of an independent insurance advisor.

Reviews and Certifications

For internal OneSpan Information Systems and Information Assets, we conduct regular internal reviews and employ continuous security monitoring. In order to provide additional assurance, OneSpan has conducted periodic independent reviews of the key components of its security program. These reviews are carried out by individuals independent of the area under review. Areas for review and the schedule for such reviews is determined based on their criticality.

For customer facing products and services, in addition to internal reviews and testing, we undergo various external reviews and certifications. Some of our products are certified under specific technical standards or industry guidelines, such as European banking regulations referred to as PSD2. In addition, our cloud platforms for SaaS solutions are audited annually by external independent auditors. The auditors review our platforms against the Service Organization Controls (SOC) 2 and ISO 27001, 27017 and 27018 standards. We receive annual certifications under these audits.

In addition, we conduct self-certification activities for those standards or regulations that are not covered by the external auditors, such as GDPR in Europe and HIPPA in the United States.

Training

In order to reduce the likelihood and impact of security incidents, OneSpan has implemented a global security awareness training program that includes mandatory security and privacy awareness training for all personnel at hire time and yearly thereafter. Additional training is be made available to personnel as required based on their role. This includes secure development training for developers, in support of OneSpan's secure development lifecycle, as well as incident response training.

In response to the various phishing attacks that often are at the root of many security breaches, and in addition to the various technical controls that are in place, OneSpan has implemented recurring phishing campaigns that target its employees at a minimum on a weekly basis to improve their ability to recognize and report phishing messages.