Koppers Statement on Confidential Information, Information Security and Data Privacy

Koppers is committed to ensuring the confidentiality, integrity and availability of data that are owned and managed by Koppers. Koppers is also committed to protecting confidential information that is shared with us by our business partners. The cybersecurity program at Koppers has been designed based on an industry standard cybersecurity framework and is aligned with local and regional compliance requirements. The cybersecurity program is reviewed periodically by an independent third-party, and the results are shared with the Board of Directors. Components of the cybersecurity roadmap are guided by the results of the independent third-party assessment. The cybersecurity program is part of the larger Enterprise Risk Management (ERM) program which is reviewed by Management and the Board of Directors on a periodic basis. Compliance with the cybersecurity program is ensured via policies, procedures, training, and systems.

Information security policies at Koppers lay out the guardrails that ensure compliance to the program. Examples of guardrails set within the information security policies at Koppers include application of the principle of least privilege when granting access, logging and monitoring activity of privileged accounts, authorized physical and logical access to information technology (IT) systems, and requiring maintenance of confidentiality of non-public information. Standard operating procedures (SOPs) ensure accuracy and completeness of various IT tasks being performed throughout the organization. SOPs include incorporating data processing agreements in contracts, commissioning and decommissioning of IT systems, granting role-based user access, patch management, and change management. Training is conducted regularly for all employees who interact with Koppers IT systems. Specialized training is also conducted for employees who deal with sensitive data. Security systems have been deployed to manage vulnerabilities within the IT environment, and periodic penetration tests validate the Koppers security posture.

IT systems are protected using various tools like multi-factor authentication (MFA), virtual private network (VPN), firewalls, end-point protection, spam and web filters, mobile device management, and privileged access management. Third-party monitoring service aids in detecting any threats or anomalies with the network. A multi-department incident response plan has been developed to facilitate a swift response in the event of a cybersecurity incident, which includes notifying the appropriate regulatory agencies. IT systems critical to the business operations have been identified and plans have been developed for a swift recovery of IT services in the event of a service failure. Koppers utilizes various IT cloud service providers. Annual security reviews of all service providers that provide critical service to the business are conducted. A cybersecurity risk assessment is conducted prior to contracting with a new IT cloud service provider providing high impact services.

Koppers has not experienced a material information security incident. An update on the cybersecurity program is provided to the Board of Directors on a quarterly basis.

3/23/2022