UFP Technologies, Inc.
Information Technology

Responsibilities

While general risk assessment and management oversight resides with the Company's Audit Committee, oversight of risks from cybersecurity threats resides with our Board of Directors ("BOD"). The BOD is formally updated on cybersecurity risks by the VP of Information Technology no less than annually. Management is responsible for assessing and managing material risks from cybersecurity threats. This responsibility primarily resides with the VP of Information Technology and his qualified team, including a dedicated Cyber Security resource. Information security risks are included in a subsection of the Company's overall risk assessment. The Corporation's executive team oversees the strategy of the Vice President of Information (VP of IT) who has primary responsibility to design and administer the policies and practices in place to protect the information, applications and hardware utilized by the Corporation to process transactions and accumulate and store data. The VP of IT also meets with external IT auditors a couple of times a year to support the audit and provide documentation of controls including those related to cybersecurity. Internal Audit of the Corporation also documents and tests the information technology general controls and policies as part of the annual control audit plan.

Insurance

The Corporation has a cybersecurity insurance policy. The SVP of Finance & Chief Financial Officer and the Vice President and Corporate Controller review all insurance policies and coverages at least annually.

Policy

The Corporation has a Cybersecurity Policy that is updated as necessary and reviewed and approved annually by the VP of IT and the SVP of Finance & CFO of the Corporation. The Cybersecurity Policy describes the practices and procedures in place that are designed to protect the critical information and technology resources of the Corporation and includes descriptions of potential threats. The Policy also includes a cyber incident response plan and specifies the professionals of the Corporation who are part of the incident response team.

Training

All new employees attend a formal training session that covers the IT Acceptable Use Policy, GDPR regulation, handling of controlled unclassified information, and insider threats and incident reporting related to the Corporation's security practices. Periodic updated training is provided to all employees.

Recent Breaches

2023 The Corporation experienced no significant cyber breaches.

2022 The Corporation experienced no significant cyber breaches.

2021 The Corporation experienced no significant cyber breaches.

The Corporation has incurred $0 net expenses related to information security breach penalties and settlements.