Standex

Progress Starts Here.™

ESG FOCUS: Cybersecurity

February 2026

Max Arets
Chief Information Officer

Message from our leaders

“The resilience of our business depends on the resilience of our IT systems.

Cybersecurity at Standex is about anticipating risks, protecting data, and empowering employees with the knowledge to act safely.

This commitment strengthens not only our operations, but also the confidence of those who work with us”.

Standex at a glance

FY25 REVENUE	FY25 OPERATING INCOME	MKT CAP as of 02.20.2026
$790M	**$94M**	**$3.12B**

~4,100 employees

53 plants & service centers

in 19 countries

Standex International Corporation is a **global industrial** growth company operating through market-leading brands in **electronics**, cutting-edge **forming technologies**, **engraving** and **scientific refrigeration**.

Standex is a public company, listed on New York Stock Exchange **since 1965** (NYSE: SXI).

Cybersecurity at the core of ESG strategy

In our industry, innovation and reliability are not built only in laboratories or plants. They also depend on our ability to **protect information, systems, and people from** constantly evolving **digital threats.**

At Standex, **cybersecurity** is not just a technical requirement: it is a **strategic pillar** to safeguard the Company's value, ensure operational continuity and maintain the trust of our stakeholders.

As digital assets have become essential to long-term value creation, cybersecurity is also a **material ESG risk**: a significant breach can disrupt operations, compromise personnel and customer data, and expose the Company to regulatory and financial consequences.

Therefore, **strong cyber governance** and **proactive risk management** are critical to building **business resilience** and meeting **stakeholder expectations**.

Cybersecurity as a priority

EXAMPLES OF WHAT WE PROTECT

DATA

- Customer & partner data - Supply chain information, technical specifications, commercial agreements, and joint project data.
- Employee data - Personal and HR-related information, including payroll, privacy, and health data.
- Sensitive business data - Financial, operational, and strategic information used across global functions.

DIGITAL ASSETS

- Intellectual property & innovation – Proprietary designs, engineering know-how, manufacturing technologies, and R&D outputs for strategic sectors (automotive, aerospace, defense).
- Product and process data – Drawings, specifications, testing results, quality records, models and production recipes.

DATA PLATFORMS

- Operational systems - IT networks, ERP systems, MES and production software, global manufacturing networks, and connected machinery.
- Digital platforms - Cloud environments, collaboration systems, databases, remote-access tools and industrial IoT devices.
- Critical business systems - Email, identity and access management, backup and recovery infrastructures.

POTENTIAL IMPACT

- **Business continuity** - Plant shutdowns, delivery delays, production disruptions.
- **Financial impact** - Direct response and insurance costs, contract losses, regulatory fines.
- **Reputation & trust** - Loss of confidence among customers, partners, investors and the public.
- **Regulatory exposure** - Notification obligations, penalties for data breaches, potential litigation.

Governance & Responsibility

1 **BOARD OF DIRECTORS** provides oversight of cybersecurity and sets priorities

2 **AUDIT COMMITTEE** oversees the strategy and the efficacy of IT controls and reports to the BoD on cybersecurity issues

3 **CYBERSECURITY COUNCIL** (comprised of Chief Information Officer, Chief Legal Officer, and Director of IT Security) oversees the execution of the cybersecurity program and policies

MANAGEMENT RESPONSIBILITIES

- CIO and Director of IT Security ensure effectiveness of access and security controls, deployment of security tools, application of policies and employee training on IT procedures
- Both are responsible for IT security strategy, its deployment and continuous improvement
- The Director of IT Applications strengthens Standex's growing digitalization efforts

REPORTING CHAIN

- Cybersecurity Council (CIO, CLO and Director of IT Security) presents to the Audit Committee quarterly updates on the status and plans for IT and IT security. Updates can be even more frequent if needed.
- Chair of the Audit Committee is immediately informed of any breach above a *de minimis* threshold and briefed on the substance of any Form 8-K filing related to a material cybersecurity incident

BOARD OVERSIGHT

- The Audit Committee reports on cybersecurity issues to the full Board after each meeting

Assessment and management of cyber risks

The three members of the Cybersecurity Council have in aggregate over 40 years of experience in assessing and managing cyber risks

Max Arets - Chief Information Officer
leads Standex's global IT and cybersecurity strategy, driving digital transformation and aligning technology with business growth.

Before joining Standex in 2024, he held senior roles at Pentair, including VP of Digital Enterprise and Senior Director of Finance Transformation.

He holds an M.Sc. in Industrial Engineering & Management from the University of Twente, completed by postgraduate studies in EDP Auditing at Vrije Universiteit Amsterdam.

Alan Glass - Chief Legal Officer
has served as Vice President and Chief Legal Officer at Standex since 2016, overseeing legal, compliance and risk management functions.

Prior to joining Standex, Glass spent 16 years leading legal, compliance, and risk functions at CIRCOR International, and earlier held internal counsel roles in aerospace/industrial companies, as well as private practice.

He holds a J.D. from Boston University and a B.A. from Cornell University.

Brian Cottle – Director of IT
has served as Director of Information Technology at Standex since 2011, bringing over 26 years of experience in audit, systems, and corporate controls.
He is responsible for leading IT operations and driving information security initiatives.

Prior to this role, he held positions in corporate audit and assurance and, earlier, in industry roles.

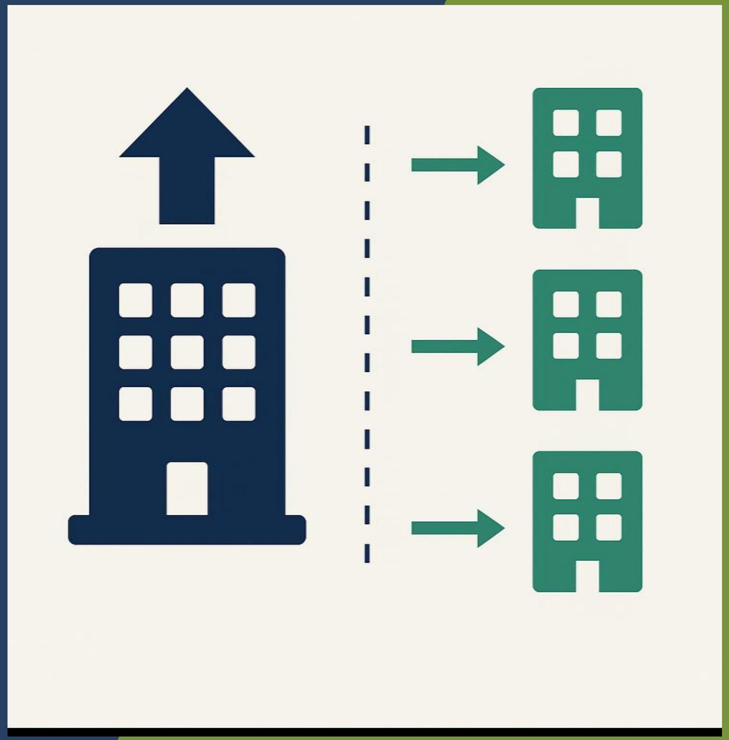
He earned a B.Sc. in Finance from Lehigh University.

Cybersecurity operating model

CORPORATE

Cybersecurity function

- Protection of external perimeter
- Penetration testing and vulnerability scanning
- Central monitoring, reporting and detection tools
- Identity & access management standards
- Global software and patching policies
- Corporate backup and recovery infrastructure



BUSINESS UNITS

- ERP, MES, and OT system security
- CRM and customer data management
- Local endpoint protection and monitoring
- Website and application security management
- Compliance with corporate cybersecurity standards
- First-level incident detection and reporting

Our Cybersecurity framework

NIST

SP 800-171

Our organization uses **NIST SP 800-171**, the federal standard governing the protection of Controlled Unclassified Information (**CUI**) within non-federal systems, as a guiding framework. This compliance ensures **stronger safeguards for sensitive technical data**, enhances trust with customers in regulated industries and supports the Company's participation in aerospace, defense and other critical supply chains. External audits are conducted to validate compliance.

800+

BitSight Score

Standex's security posture is also externally assessed through BitSight, one of the leading providers of independent **cybersecurity ratings**.
The strong **BitSight score achieved in August 2025 (800+)** confirms the **effectiveness of the controls in place** – including vulnerability management, patching cadence, endpoint protection, and incident response – while providing quantitative assurance to stakeholders.

Risk Management

***Cybersecurity risk management** is an integral part of our broader **Enterprise Risk Management** (ERM) framework. We view cybersecurity not simply as a technical issue, but as a **core business risk**.*

Our approach is based on continuous **identification, assessment, and mitigation of threats** across the Company's global operations. Our internal committee **monitors and evaluates evolving risks** – from malware and ransomware to phishing, denial-of-service attacks, and third-party vulnerabilities – and implements appropriate controls to reduce exposure.

We apply a **layered defense strategy** that combines technical safeguards, administrative controls, and human awareness. This includes network and endpoint protection, strict access management, regular software patching, and data encryption, as well as clearly defined security policies and mandatory training for all employees.

In the event of a security incident, a **formal incident response program** ensures swift detection, escalation, containment, and recovery. These procedures are **regularly tested and updated**, enabling the Company to minimize disruption and protect critical assets. In May FY25, Standex senior leadership also participated in a **tabletop ransomware simulation**, testing escalation, communication and response procedures as part of our **continuous improvement program**.

Cyber risks **are reviewed and reported regularly** to the Board, ensuring **alignement with business priorities** and **evolving regulatory requirements**.

Such structured oversight allows cybersecurity to be managed with the same rigor and accountability as financial, operational, and strategic risks, while reinforcing our **commitment to safeguarding the Company's people, data and technology.**

Training & Awareness

1 **Mandatory training -** All employees with access to IT systems complete mandatory cybersecurity training during onboarding and twice per year. Training covers core topics, including phishing and social engineering, password hygiene, data handling, mobile security, and emerging risks such as AI-enabled threats and deepfakes.

2 **Policy acknowledgment -** Every employee signs the Company's cybersecurity policy, confirming awareness of expectations and responsibilities. Beginning 2026 , the members of the IT team will also be required to sign an additional attestation related to the handling of sensitive data and elevated-access protocols.

3 **Phishing simulations and education -** we conduct semi-annual phishing simulations to test employee readiness and reinforce safe behaviors. Results are monitored and shared with managers to support targeted coaching and continuous improvement. Employees also receive regular security reminders, updates on evolving threats, and guidance on best practices for protecting company and customer data.

4 **External validation -** Standex leverages independent third parties for annual audits and penetration testing, strengthening oversight and validating the effectiveness of internal controls. The Cybersecurity Audit Plan is updated each year and presented to the Board in July. Third-party assessments are conducted for critical suppliers or upon request from the leadership team.

In FY25, 100% of the tested employees completed the phishing simulation, of which 98% on time

Metrics - FY25 *(1 July 2024 – 30 June 2025)*

15

Info security **incidents** in 3 years (FY23 –FY25)

0

Penalties/ settlements in relation to info security **incidents**

0

Fees spent on **incidents** as % of revenues in FY25

~ 16%

Cybersecurity budget / Total IT budget

Over the last few years, we have experienced a small number of minor cyber incidents. To date, none of them have been material or had a material adverse effect on our operations or financials. This is reflected in a zero amount of fees spent on incidents as a percentage of total revenues and in a zero amount for penalties or settlement paid in FY25.

In addition, as far as we know, Standex has not experienced any third-party information security breaches.

At Standex, we are keeping our guard up. As poof of that, we stick to a **high incidence of cybersecurity expenditure** in the total IT budget.

We also maintain a **cybersecurity insurance** to mitigate any potential impact of cybercrime activities.

Standex®

23 Keewaydin Drive | Suite 300 | Salem, New Hampshire 03079 | +1.603.893.9701 | standex.com

For further information please contact:

PAOLO MACCHI
President of ESG Council
pmacchi@standex.com