Cybersecurity Updates

For Discussion
PNE Board of Directors
January 29, 2026

Cybersecurity

Why This Matters?

- Cybersecurity protects the PNE's people, information, and ability to operate.

- The PNE relies heavily on digital systems to:
  - Deliver events and programs at scale
  - Process high volumes of transactions
  - Protect employee, partner, and public information

- Strengthening cybersecurity helps us to:
  - Safeguard personal and financial data
  - Reduce the risk of service disruption during major events
  - Meet regulatory expectations
  - Maintain public trust and organizational resilience

Cybersecurity Initiatives - Overview

- **Managed Detection & Response (MDR):** Partnered for advanced 24/7 proactive monitoring and automated response within the Microsoft 365 environment.
- **Strengthened Network Protection**
  Continuing upgrade of firewall infrastructure with new technology from Cisco, scheduled for implementation in early 2026, to further protect our systems and data.
- **Payment Security Compliance Achieved**
  Successfully completed **PCI DSS certification** in December 2025,providing ongoing annual confirmation that our payment systems meet industry standards for protecting customer financial information.
- **Clear Cybersecurity Risk Oversight**
  We are developing a Cybersecurity Risk Register aligned with the National Institute of Standards and Technology Cybersecurity Framework to ensure risks are clearly identified, tracked, and managed at an enterprise level.

Cybersecurity Incident Readiness

Tabletop Exercises

- **Purpose**

  To prepare leaders and staff to respond effectively to a simulated cyber incident, with a focus on clear communication and timely decision-making.

- **Why This Matters**

  These exercises allow the organization to test and improve response plans in a controlled setting—without the risk of a real data breach or service disruption.

- **FIFA Readiness**

  Multiparty tabletop exercises are scheduled for April–May to ensure the organization is prepared to maintain secure and reliable operations during high-profile international events, while protecting sensitive data.

Key Cyber Risks & How We Manage Them

- **1. Email-Based Threats (Phishing & Malware)**
  Risk: Fraudulent emails or malicious links that target staff.
  Mitigation: 24/7 system monitoring and ongoing staff awareness training.

- **2. Unauthorized Network Access**
  Risk: Attempts to gain access to internal systems.
  Mitigation: Deployment of next generation firewall technology

- **3. Payment & Regulatory Compliance**
  Risk: Noncompliance with payment security requirements.
  Mitigation: Annual payment security assessments and ongoing compliance monitoring.

- **4. Incident Response Readiness**
  Risk: Delayed or uncoordinated response to a cyber incident.
  Mitigation: Regular tabletop exercises

Governance & Future Roadmap

- **Board Oversight**
  Cybersecurity is treated as a core organizational risk, with Board oversight focused on aligning investments and priorities with a formal risk management framework.
- **Strategic Evaluation**
  Leadership will continue to assess and prioritize future cybersecurity investments to address evolving risks and organizational needs.
- **Looking Ahead**
  Cybersecurity is an ongoing commitment. The PNE is committed to a continuous cycle of improvement, including regular system updates, readiness exercises, and routine reporting to the Board of Directors.