LINEASECURE

Navigating Cyber Risk and Board Responsibility

Federated Retirement Plan Board
2025 Cybersecurity Workshop

Los Angeles | Washington DC | Toronto

Peter Dewar, CISSP, CDPSE, CAPPP

President, Linea Secure

- Founded Linea Secure in 2018
- Over **25 years of experience** in I.T. and cybersecurity.
- 15 years in public pension fund security
- Former **Chief Technology Officer of District of Columbia Retirement Board (DCRB)**
- Extensive work with Pension Boards on improving cybersecurity awareness

Jake Long

Senior Consultant

- Over **14 years of experience** in the public pension industry, leading complex implementation projects with both business and technical oversight
- Former **Software Development and Data Conversion Manager** for a pension administration software provider.
- Highly experienced with Microsoft technologies, including C#, .NET, SQL, Azure DevOps, and SQL Management Studio
- Actively building cybersecurity expertise through work on policy development, secure code reviews, and independent assessments of internal and third-party risks

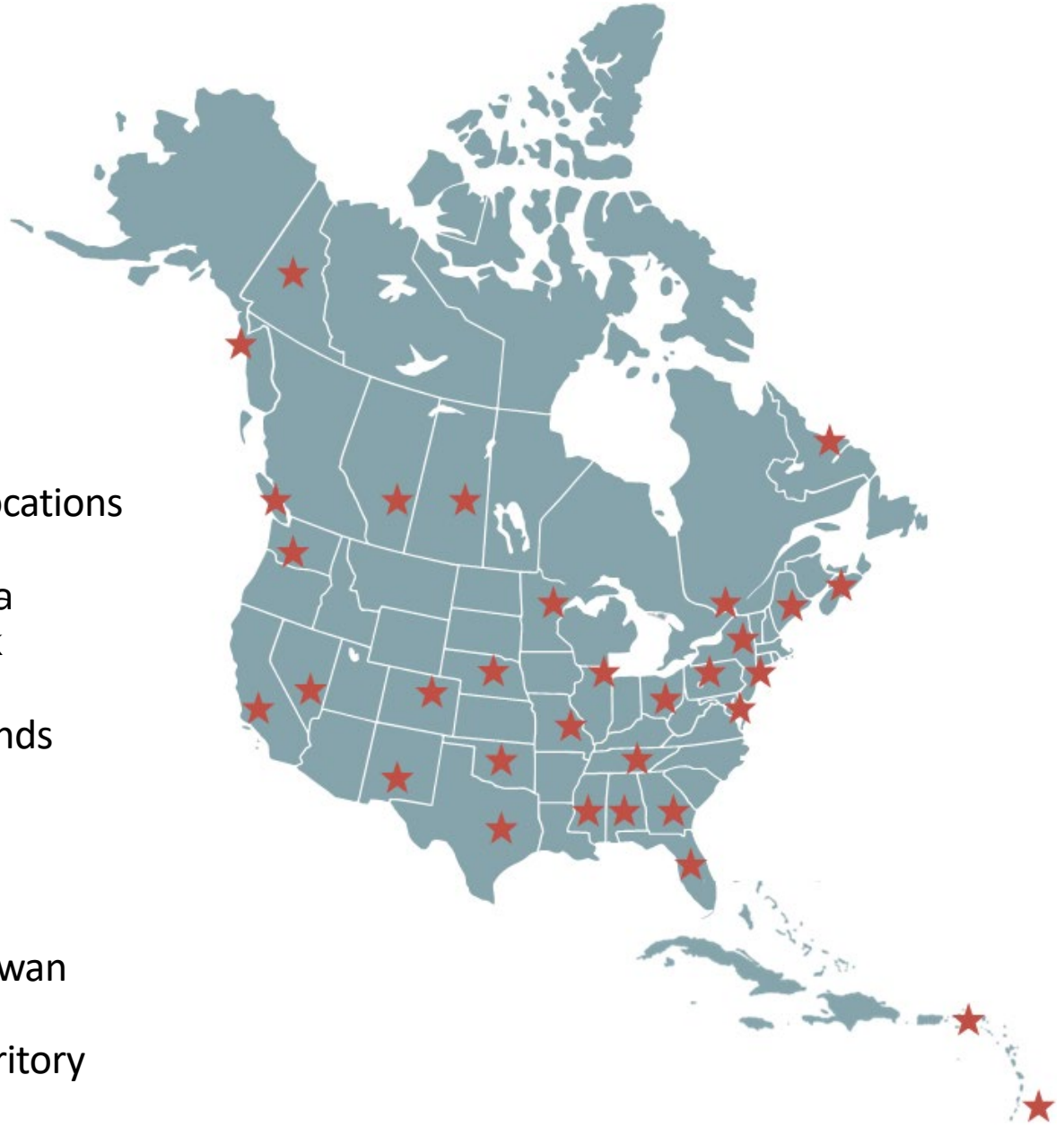
Linea Solutions - Who we are

Business Focus – National Insurance Schemes, Pension, Workers' Compensation, and Insurance Consulting

- Offices in Los Angeles, Washington DC, and Toronto
- 150+ staff members
- 120+ clients
- Provide **business and technical assessments, project management specialists and change management specialists,** assisting in all phases of business and technology transformation
- Cybersecurity & Data as key focus areas (50+ cyber clients, 15+ data)

Key Client Locations

- California
- New York
- Barbados
- Virgin Islands
- Alaska
- Hawaii
- Texas
- Florida
- Saskatchewan
- Manitoba
- Yukon Territory



Services

Strategy

Assessments

Modernization Readiness

Technical Services

Procurements

Transformation

Change Management

Business Process Reengineering

Training

Cyber Best Practices

IT Service Management

Data Migration & Cleansing

Implementation

Project Management

External System Integration

QA & Testing

BA Support

IV&V

Data Management

Linea Secure Overview

- Linea Secure is the cybersecurity division of Linea Solutions, a pension IT consulting company **serving the industry for over 2 decades**
- Offices in Washington DC, Los Angeles, Toronto
- We use **NIST as our cybersecurity framework**, customized for pension
- We have over 120 benefits clients and have provided **cybersecurity services to over 50 public pension clients** in the last 7 years

Agenda

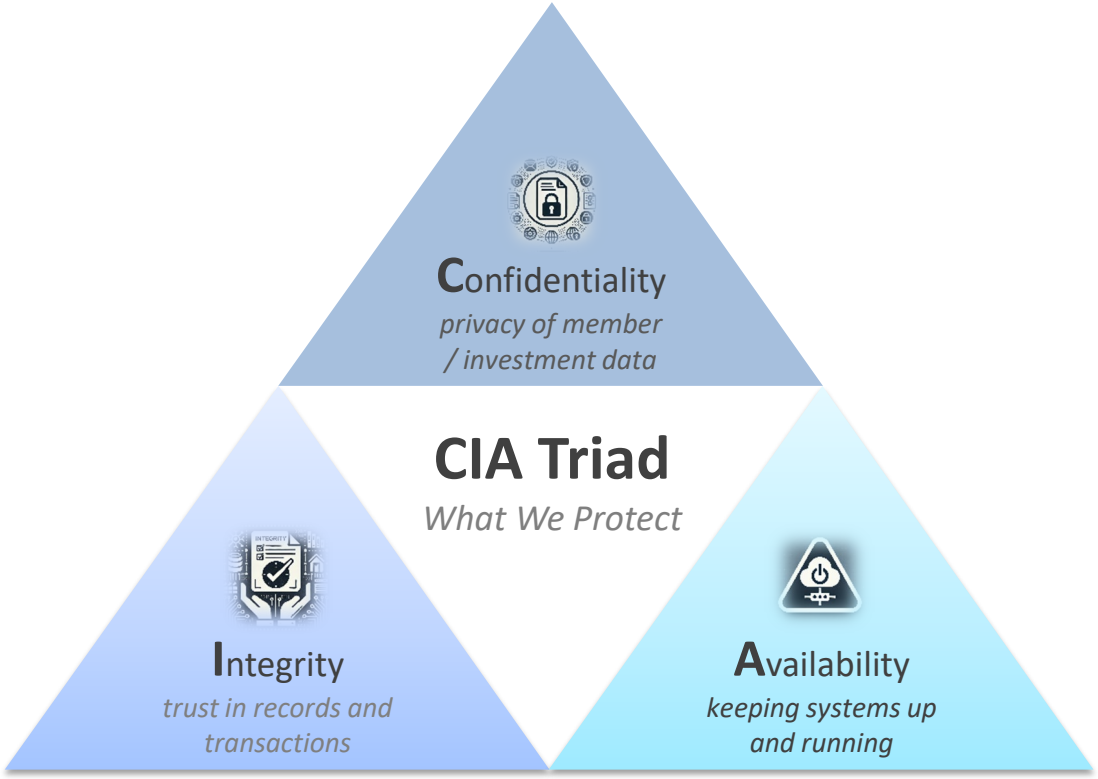
- **Recognizing Today's Cyber Threats and your Risk Exposure**
- **Understanding the Board's Role in Cyber Oversight**
- **Safeguarding ORS – and Protecting Yourself**

Recognizing Today's Cyber Threats and your Risk Exposure

Public pension systems like ORS face growing cyber threats that target sensitive data, critical operations, and third-party relationships.

Cybersecurity

Cybersecurity means protecting ORS's systems and data, so they remain available, accurate, and private — even during a cyberattack.



Big Picture: Why Should Cyber Threats Matter to you

Public pension funds are high-value targets.

- **Personally Identifiable Information (PII)** – Names, SSNs, dates of birth, addresses
- **Benefit Payment & Banking Details** – Direct deposit information, payroll processing systems
- **Financial & Investment Assets** – Large fund balances, vendor payment workflows, ACH/wire access

The threat landscape is rapidly evolving.

- **Increased frequency and complexity** – Threat actors use automation, AI, and stealth tactics to bypass defenses
- **Ransomware is widespread** – Disrupts operations, locks critical data, and demands payment
- **Social engineering is targeting people, not just systems** – Phishing, spoofed emails, and impersonation

ORS operates in a complex digital environment.

- **Cloud-based Services + 3rd Party Platforms** – Expand attack surface and introduce vendor-related risks
- **Broad System Access** – Trustees, employees, and 3rd-party service providers may interact with sensitive data
- **Hybrid work models** – Working from home or on unmanaged networks can open the door to cyber threats

Common Threats Targeting Pension Funds

Social Engineering & Phishing
Deceptive emails or messages trick staff or trustees into clicking links or revealing credentials.

Ransomware Attacks
Encrypts critical systems and demands payment, potentially halting mission critical pension operations like benefit payroll.

Insider Threats
Employees or vendors may accidentally or intentionally expose data or bypass ORS's security controls.

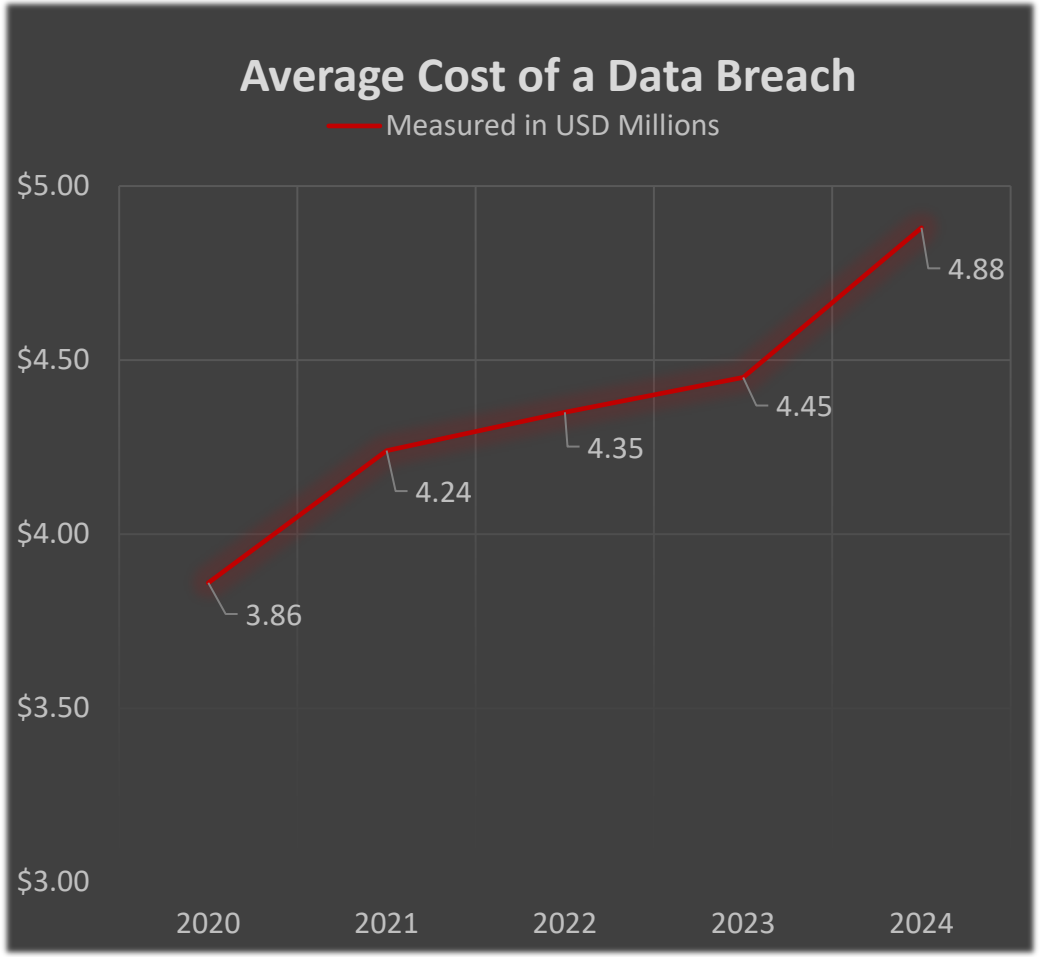
Business Email Compromise (BEC)
Attackers use fake or compromised emails to trick recipients into taking harmful actions, such as approving transactions or sharing sensitive information.

Third-Party/Vendor Breaches
A breach at an external provider can expose sensitive data or disrupt core pension services.

Credential Theft
Stolen or reused passwords allow attackers to access systems and sensitive information.

The Cost of Compromise

- Cyber attacks are **expensive**, with the average cost of a data breach now exceeding **$4.8 million,** up 10% from last year!
- **Speed of detection is critical.** Breaches involving stolen credentials take an average of **292 days** (~10 months) to identify and contain!
- **35% of breaches involve "shadow data"** — sensitive info stored in poorly tracked locations like personal cloud drives, test environments, or old file shares.
- **Strong cyber hygiene, insurance coverage, and third-party due diligence** are essential layers of defense for ORS.



***Source**: IBM Cost of a Data Breach Report 2024 (www.ibm.com/reports/data-breach)*

Understanding Key Sources of Cyber Risk

Benefit Administration

- Member Services
- Employer Reporting
- Benefit Payroll
- Document Management
- Communications

Support Operations

- 3rd Party Vendors
- Legal & Regulatory Requirements
- Accounting & Audit
- Application Support
- Network & Infra Management

Core Operations

Board Operations

- Board Meetings
- Document Handling / Sharing
- Election Procedures

Investment Operations

- Investment Managers
- Compliance
- Reporting
- Custodial Bank

Understanding the Board’s Role in Cyber Oversight

Trustees play a vital role in overseeing cybersecurity risks, asking the right questions, and ensuring the organization is prepared to respond.

Why Cyber Oversight Starts in the Boardroom

- Cybersecurity is a **governance and fiduciary responsibility**.
- **Cybersecurity is a strategic risk, not just an IT issue.** Threats impact fund assets, operations, compliance, and public trust.
- Regulators and stakeholders increasingly expect Boards to be **informed and engaged** in cyber planning and incident response.
- Trustees do not need technical expertise but strengthen the fund's security posture by **asking the right questions.**

Key Considerations

- ✓ **Data Protection**: How is sensitive member data and fund information secured?
- ✓ **Third-Party Risk**: How is ORS's information shared with key vendors (PAS, actuaries, investment managers)?
- ✓ **Incident Response**: What processes and tools are in place if something goes wrong? How do we recover and how long will it take?
- ✓ **Staff Training & Policies**: How often are staff being trained and is the training effective? Are security policies up-to-date and reviewed by the appropriate personnel?
- ✓ **Secure Communications**: How are sensitive materials accessed and shared securely?

Safeguarding ORS – and Protecting Yourself

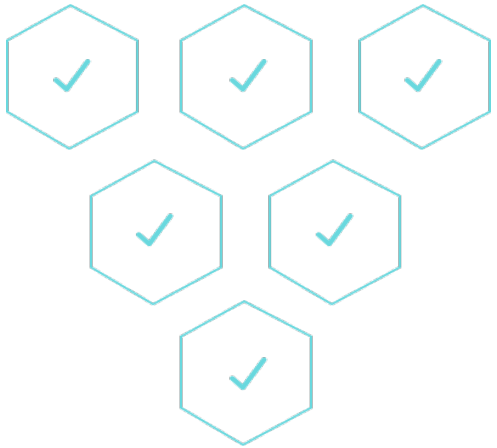
Your role: Oversight, awareness, and informed decision-making

NIST Cybersecurity Framework (CSF)

How We Manage Risk

How can you protect ORS…and yourself?

- **Use Strong, Unique Passwords** — best first line of defense
- **Turn On Multi-Factor Authentication (MFA)** — proven safeguard against account takeovers
- **Access Board Docs on Trusted Platforms** — avoid using personal email, storage, and public Wi-Fi
- **Stay Alert for Phishing Scams** — slow down, always verify before clicking or downloading
- **Know the Incident Response Plan (IRP)** — be ready to support leadership decisions if activated
- **Promote Transparency**— steady, open leadership builds trust during an incident
- **Ask Questions** — if something feels off (don’t assume IT already knows)



Thank you for your time and let us know if you have any additional questions

LINEASECURE

Email

pdewar@lineasecure.com

Web

www.lineasecure.com

Phone

703-850-4100