LINEASECURE

Navigating Cyber Risk and Board Responsibility

2025 Board Cybersecurity Workshop

Los Angeles | Washington DC | Toronto

Peter Dewar, CISSP, CDPSE, CAPPP

President, Linea Secure

Project Role: Executive Oversight

- 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

Project Role: Engagement Manager

- 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

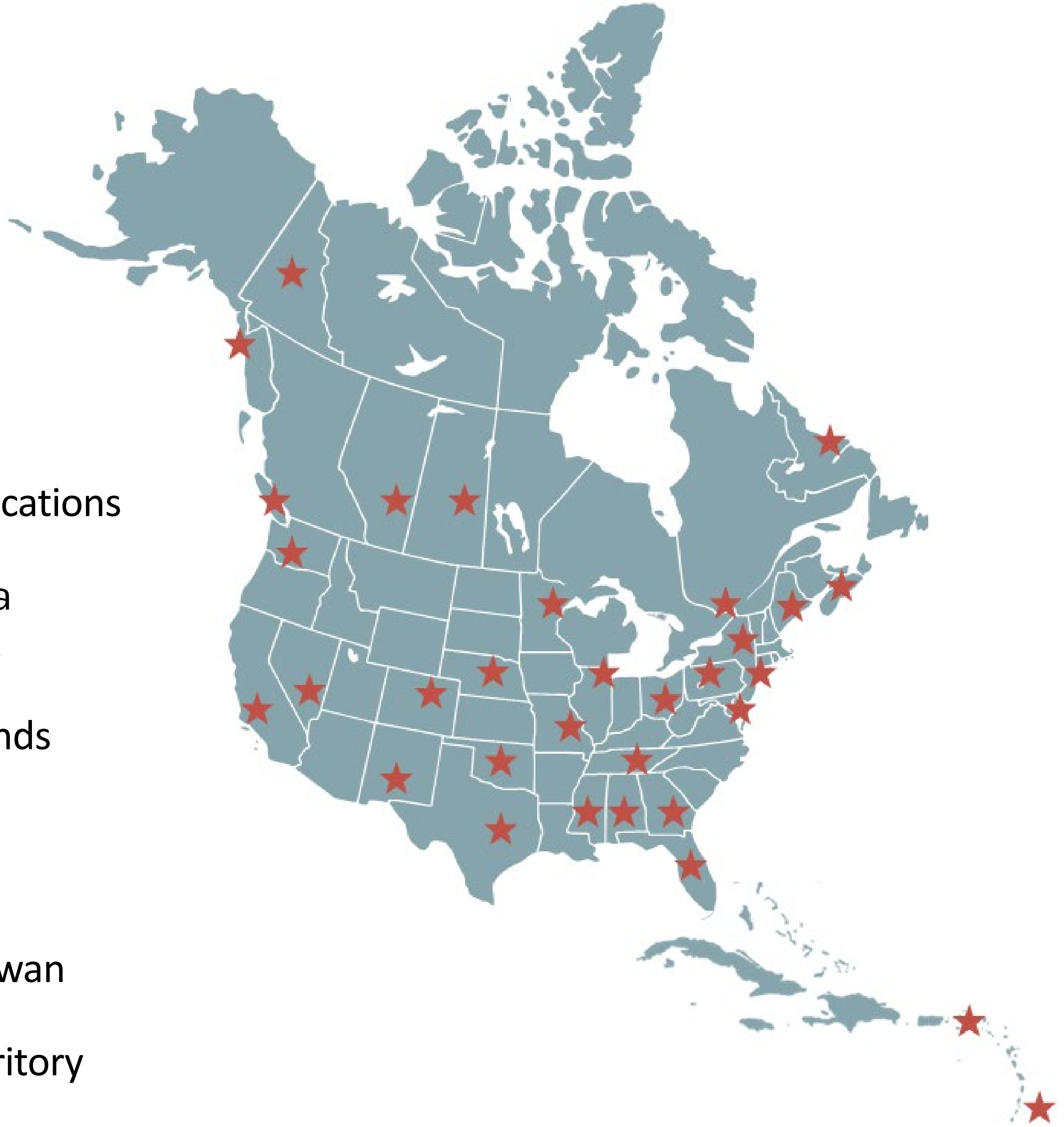
Linea Solutions - Who we are

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

LINEASECURE

- 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

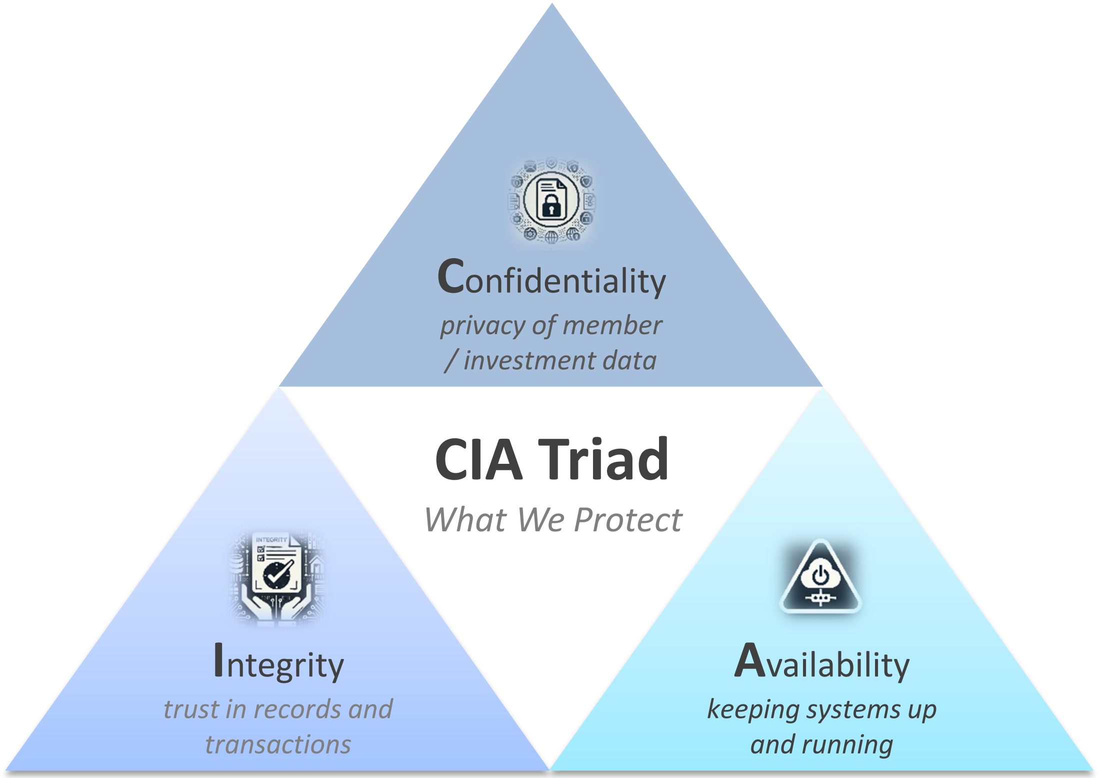
- Recognizing Today's Cyber Threats and your Risk Exposure
- Understanding the Board's Role in Cyber Oversight
- Safeguarding SJ ORS – and Protecting Yourself

Recognizing Today’s Cyber Threats and your Risk Exposure

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

Cybersecurity

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



Confidentiality

privacy of member / investment data

CIA Triad

What We Protect

Integrity

trust in records and transactions

Availability

keeping systems up and running

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

SJ 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.

Insider Threats

Employees or vendors may accidentally or intentionally expose data or bypass SJ ORS’s security controls.

Third-Party/Vendor Breaches

A breach at an external provider can expose sensitive data or disrupt core pension services.

Ransomware Attacks

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

Business Email Compromise (BEC)

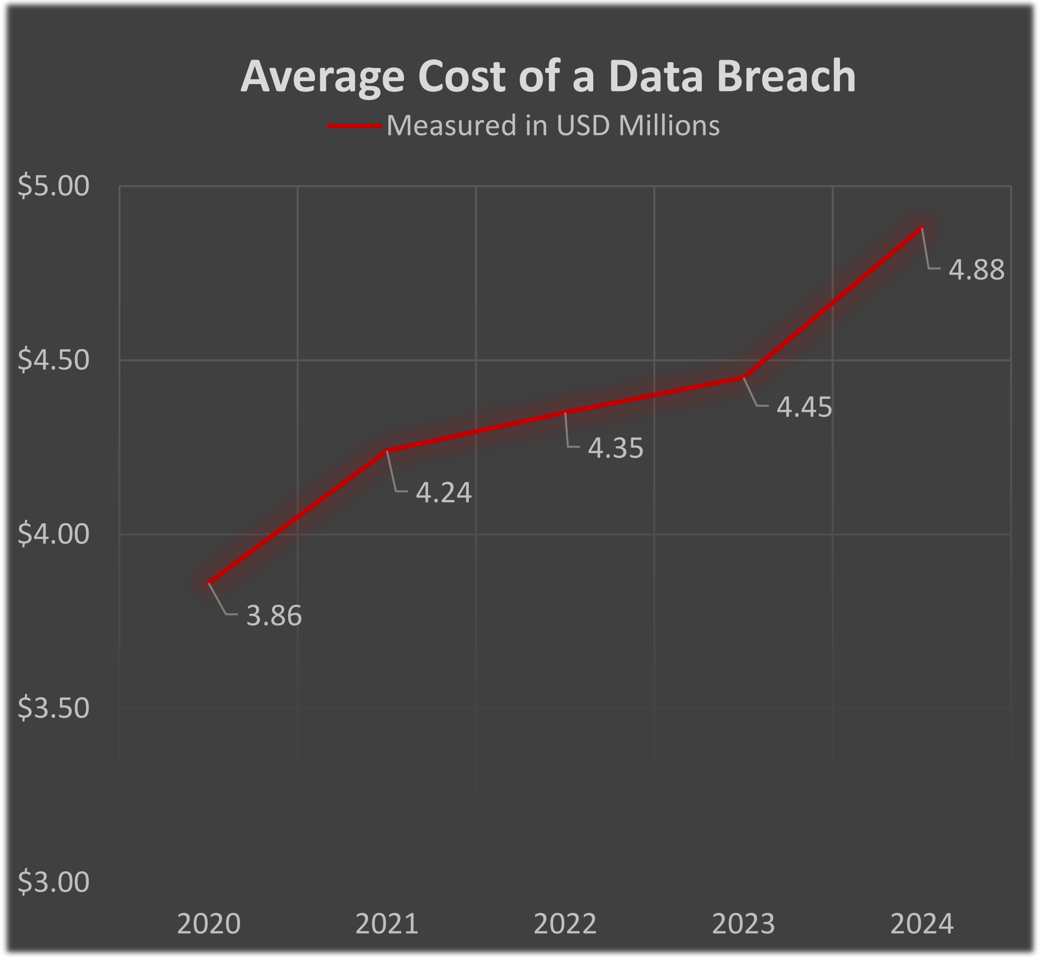
Attackers use fake or compromised emails to trick recipients into taking harmful actions, such as approving transactions or sharing sensitive information.

Credential Theft

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

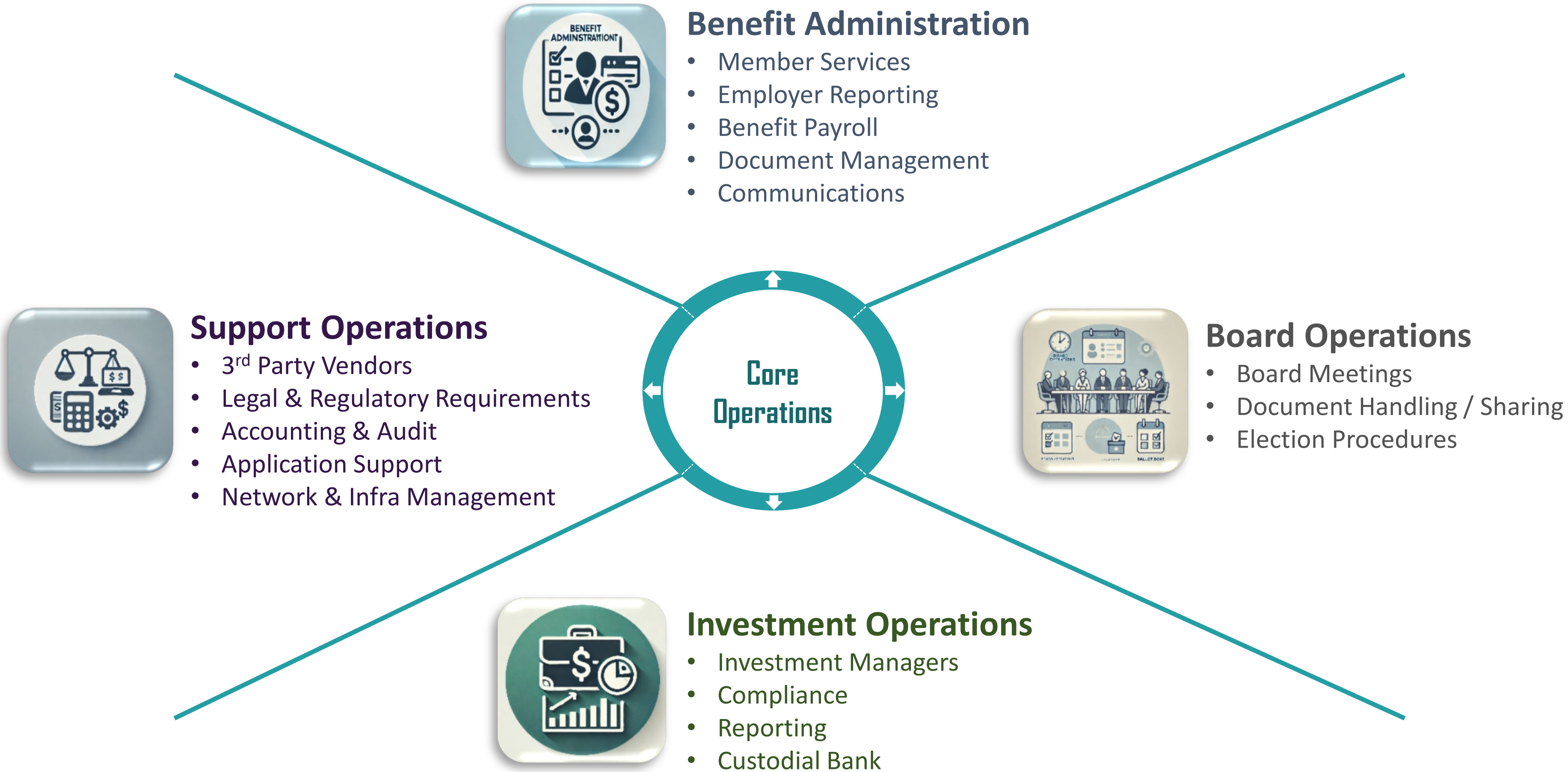
The Cost of Compromise

- 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 SJ 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

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

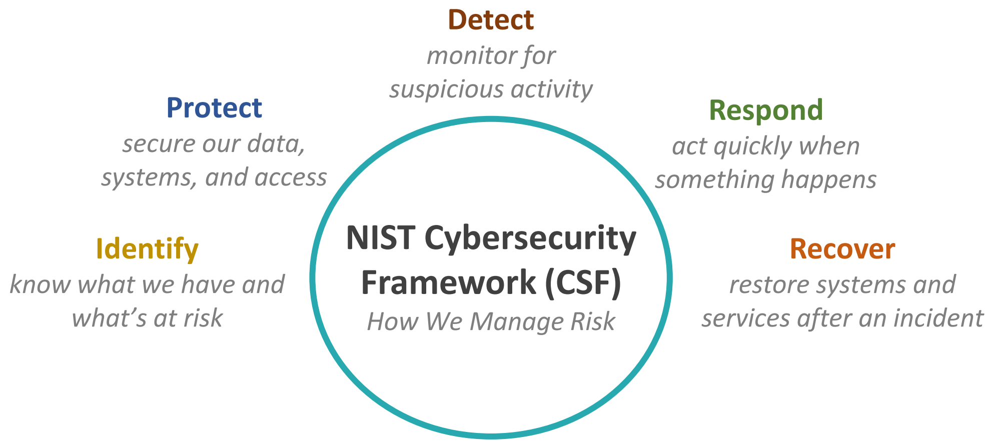
- Cybersecurity is a **governance and fiduciary responsibility**.
- **Cybersecurity is a strategic risk, not just an IT issue.** Threats impact fund assets, operations, compliance, and public trust.
- Regulators and stakeholders increasingly expect Boards to be **informed and engaged** in cyber planning 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 SJ 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 SJ ORS – and Protecting Yourself

Protecting SJ ORS starts with strong organizational controls and smart personal cybersecurity habits, especially at the Board level.



Detect
monitor for suspicious activity

Protect
secure our data, systems, and access

Respond
act quickly when something happens

Identify
know what we have and what's at risk

NIST Cybersecurity Framework (CSF)
How We Manage Risk

Recover
restore systems and services after an incident

IDENTIFY: What needs to be protected?

Identify

Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities

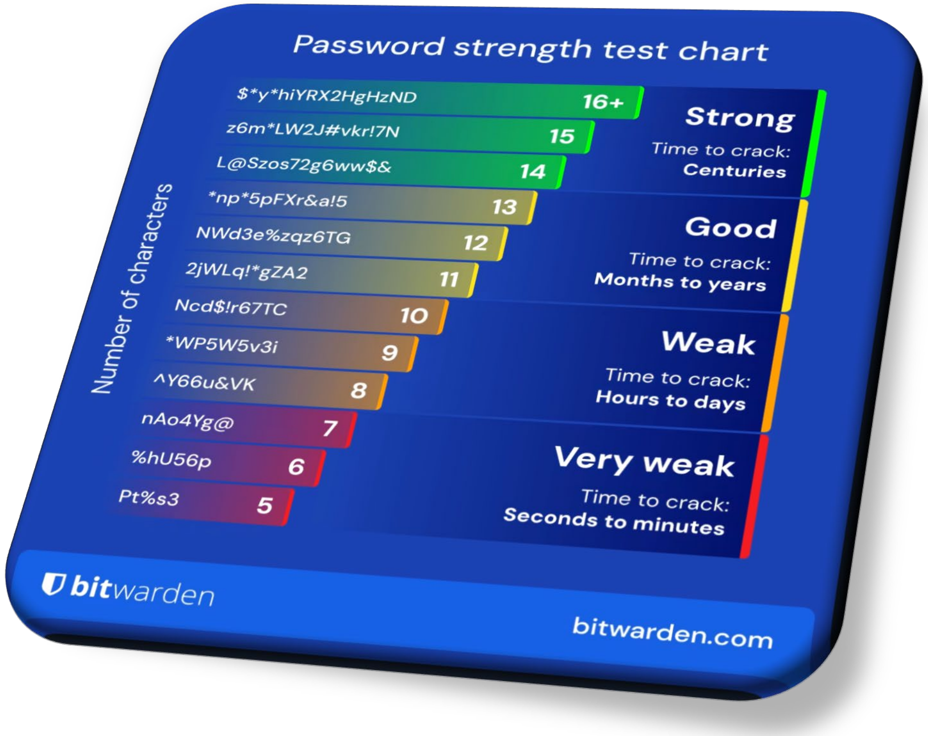
- ✓ **Member Data** – Personal info, retirement eligibility, health information, payment details
- ✓ **Financial Systems** – Contribution records, payroll systems, investment transactions
- ✓ **Board & Legal Documents** – Meeting materials, legal opinions, contracts
- ✓ **Internal Systems** – Pension administration, document management, reporting platforms
- ✓ **Third-Party Access Points** – Vendors, actuaries, custodial banks, and self-service portals
- ✓ **High-Privilege Accounts** – Admin credentials, finance access, trustee portals

PROTECT: Prevent Incidents Before they Occur

Protect

Develop and implement appropriate safeguards to ensure delivery of critical services

- ✓ Use **strong, unique passwords** for all board-related accounts
- ✓ **Avoid** accessing board materials from personal emails or unsecured Wi-Fi (without VPN)
- ✓ Only use **secure communication platforms** provided by your organization
- ✓ **Enable Multi-Factor Authentication (MFA)** on devices and apps used for board materials



DETECT: Spot Red Flags Early

Detect

Develop and implement appropriate activities to identify the occurrence of a cybersecurity event

✓ **Be alert** of common red flags and **learn** the signs of phishing, spoofing, or other social engineering attack methods

- Urgent or unusual requests via email or text
- Emails that appear to be from staff, but have typos, invalid email addresses, or unexpected attachments or links
- Unexpected login notifications or MFA prompts
- Documents shared outside normal communication channels

✓ **Trust your instincts** — if something feels off, it probably is

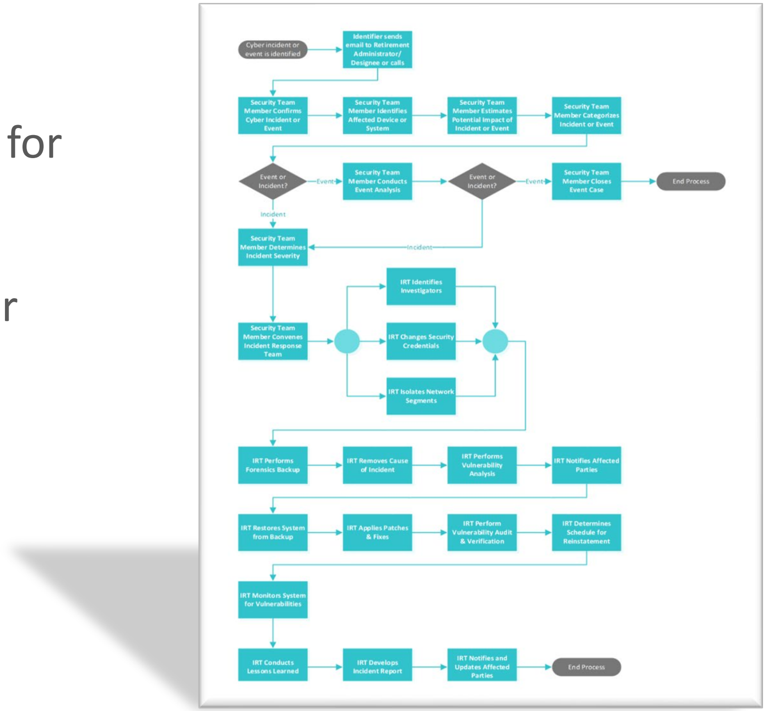
✓ **Report suspicious activity immediately** — don't assume IT already knows

RESPOND: Act Quickly if Something Goes Wrong

Respond

Develop and implement actions to take when a risk is detected

- ✓ **Know what to do** if your device is compromised or you fall for a phishing attempt
- ✓ **Be ready to act if needed** — the board may be called on for decisions during a serious incident
- ✓ If your organization has an **Incident Response Plan**, your awareness and transparency help make it effective



Cyber incident or event is identified
Identifier sends email to Retirement Administrator/ Designee or calls
Security Team Member Confirms Cyber Incident or Event
Security Team Member Identifies Affected Device or System
Security Team Member Estimates Potential Impact of Incident or Event
Security Team Member Categorizes Incident or Event
Event or Incident?
Event
Security Team Member Conducts Event Analysis
Event or Incident?
Event
Security Team Member Closes Event Case
End Process
Incident
Incident
Security Team Member Determines Incident Severity
Security Team Member Convenes Incident Response Team
IRT Identifies Investigators
IRT Changes Security Credentials
IRT Isolates Network Segments
IRT Performs Forensics Backup
IRT Removes Cause of Incident
IRT Performs Vulnerability Analysis
IRT Notifies Affected Parties
IRT Restores System from Backup
IRT Applies Patches & Fixes
IRT Perform Vulnerability Audit & Verification
IRT Determines Schedule for Reinstatement
IRT Monitors System for Vulnerabilities
IRT Conducts Lessons Learned
IRT Develops Incident Report
IRT Notifies and Updates Affected Parties
End Process

RECOVER: Support Long-Term Resilience

Recover

Implement procedures to recover from a cybersecurity event

- ✓ Trustees play a role in helping maintain public confidence during a cyber incident
  - ✓ Demonstrate calm & informed leadership
  - ✓ Encourage transparency & clear communication
  - ✓ Avoid speculation / stick to the facts
  - ✓ Be available and engaged
  - ✓ Focus on long-term stability

- ✓ Understanding recovery efforts helps inform funding and oversight decisions
  - ✓ Drives funding decisions
  - ✓ Informs future investments (systems, vendors, staffing)
  - ✓ Supports accountability (what worked / didn't work and why?)
  - ✓ Guides policy and procedure improvements

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

LINEASECURE

Email	Web	Phone
pdewar@lineasecure.com	www.lineasecure.com	703-850-4100