Cybersecurity

Lessons Learned from Failures and Successes

Chief Officers Summit, June 21, 2023
Introductions

• Jeff Mills – VP and Senior Consultant with Segal’s Administration and Technology Consulting Practice

• Bill Betts, Executive Director with Missouri Local Government Employees Retirement System

• Peter Chenoweth, Levi, Ray & Shoup Retirement Solutions
Today’s Topics – From 3 Perspectives

1. Consultant
   • Threat landscape
   • A recent pension data breach
   • Common Assessment Findings

2. Executive Director
   • Real World Examples
   • Incident Response
   • Things to consider

3. Pension Software Vendor
   • Software vendor expectations
   • Threats explored with customers
   • Key remediation Efforts
A Recent Breach in the News

- 3/31 – Capita Reports Technical Issue (9 days after intrusion)
- 4/3 – Recognized as a Cyber Attack with “Black Basta” taking responsibility (Qbot malware)
- 5/3-11 – told clients pensioner data had been exposed
- Mid May – Second Breach identified
  - Technical Documentation
  - Other financial data of clients

Capita Data Breach Affects Britain's Largest Pension Fund

Capita CEO Jon Lewis told The Sunday Times for a report published April 9 that his firm's response to the hack attack “will go down as a case history for how to deal with a sophisticated cyberattack.”
Potential Lessons From This Breach

**Protect Systems**
- System Documentation (e.g. schematics, server details, results from assessments)
- Malware Detection
- Intrusion Detection
- Data Loss Prevention

**Protect the Organization**
- Business Partner Agreements (e.g. PAS Vendors, Actuaries, Consultants, etc.)
- Third Party Vendor Assessments

**Incident Response Planning**
- Analysis and Assessment
- Communications / Pre-Written
- Table-Top Exercises
Common Findings in Segal NIST Assessments

- No Incident Response Plan
- No Ongoing Training
- No Data Encryption
- No Data Classification
- Allowed use of USB Drives
Real World Examples

SHARK WEEK

LEGACY E-MAIL
Shark Week Incident Response

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Lessons Learned
Things to Consider

PREPARATION IS KEY

RESOURCES MATTER

INFINITE GAME
Expectations of your PAS software vendors

- Transparency
- Address all questions and concerns
- Best Practices
- Application Programming and Infrastructure
- Insistence on regular assessments both application and network
- Vulnerability Assessments
- SOC 2
- Certifications
Typical threats LRS customers have encountered

• Member and Beneficiary identity impersonation through self-service portals.

• Green Dot Bank payroll redirection.

• Ransomware and shared infrastructure.
Key lessons learned and remediation efforts

• Multi-factor authentication.

• Encryption at every level.

• Staff education; phishing education, awareness of scams.

• Security, business continuance, and recovery policies and procedures.

• Have a plan. Practice that plan.
Key Takeaways
Questions and Other Experiences