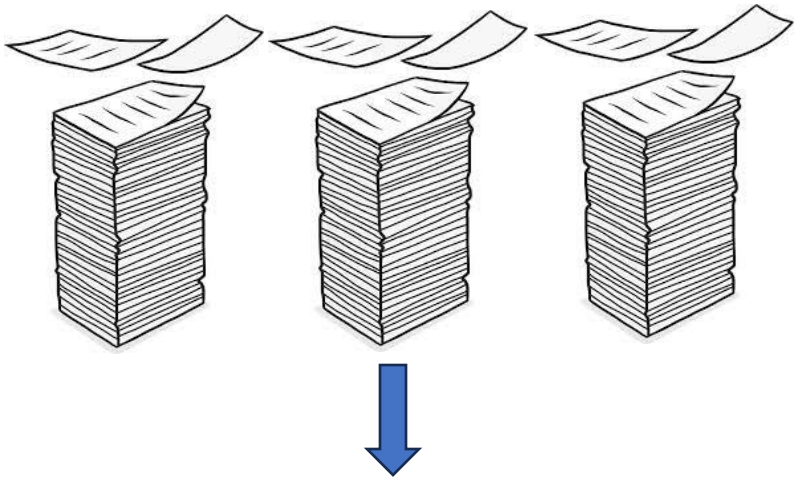
TeamCare Through The Years - Today's "State Of The Art" Health Fund

LIVING IN AN ELECTRONIC WORLD – FOLLOW A CLAIM



- We have a come a very long way over the decades. All claims used to be mailed to us in paper form, and an Adjuster would process each one.
- Today all claims are received electronically via our partnership with Blue Cross, and about 90% get processed via automation without any human intervention.
- We process approximately 7 million claims a year.

LIVING IN AN ELECTRONIC WORLD – FOLLOW A CLAIM

Services rendered at provider's office/hospital

Provider sends claim to their local Blue Cross host plan

Blue Cross host sends claim to Blue Cross IL

Blue Cross IL sends claim to the Fund

The Fund applies eligibility & benefits (90% automation)

The Fund sends claim back to Blue Cross IL & sends the Member EOB

Blue Cross IL sends claim to the host plan

The host plan sends EOB and payment to the Provider

The Provider sends a bill to the Member, if applicable

Electronic Data Interchange

TEAMCARE® CENTRAL STATES PENSION FUND

SUMMIT 2025

Cybersecurity and Protecting Member Data

Tom Forkenbrock – Chief Information Security Officer

Mark Schneider – HIPAA Security Officer

AGENDA

- Department of Labor Recommendations and Guidelines
- Examples of How Data is Compromised
- How Do We Protect Your Data?
- Central States Funds Security Practices
- How Does This Help You?
- What Happens If…

Department of Labor Recommendations

- On April 14, 2021, the U.S. Department of Labor (DOL) announced new guidance for plan sponsors, plan fiduciaries, record keepers, plan service providers and plan participants on best practices and tips for maintaining cybersecurity, including 12 guidelines on how to protect the retirement benefits of America's workers. Much of the guidance is directed at plan sponsors and fiduciaries regulated by the Employee Retirement Income Security Act (ERISA), and plan participants and beneficiaries.
- Without sufficient protections, participants and assets within these plans may be at risk from both internal and external cybersecurity threats. ERISA requires plan fiduciaries to take appropriate precautionary measures to mitigate these risks.
- The purpose for this policy is to provide an overview, based on this DOL guidance, of the cybersecurity practices and controls deployed by Central States Funds to mitigate cybersecurity risks and protect our organization and our members from internal and external threats.

https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/best-practices.pdf

DOL Guidelines

1. Have a formal, well documented cybersecurity program
2. Conduct prudent annual risk assessments
3. Have a reliable annual third-party audit of security controls
4. Clearly define and assign information security roles and responsibilities
5. Have strong access control procedures
6. Ensure that cloud/3rd-party hosted assets are reviewed and assessed externally
7. Conduct periodic cybersecurity awareness training
8. Implement and manage a secure system development life cycle (SDLC) program
9. Have an effective resiliency program addressing business continuity, disaster recovery, and incident response
10. Encrypt sensitive data, stored and in transit
11. Implement strong technical controls in accordance with best security practices
12. Appropriately respond to any past cybersecurity incidents

Examples of How Data is Compromised

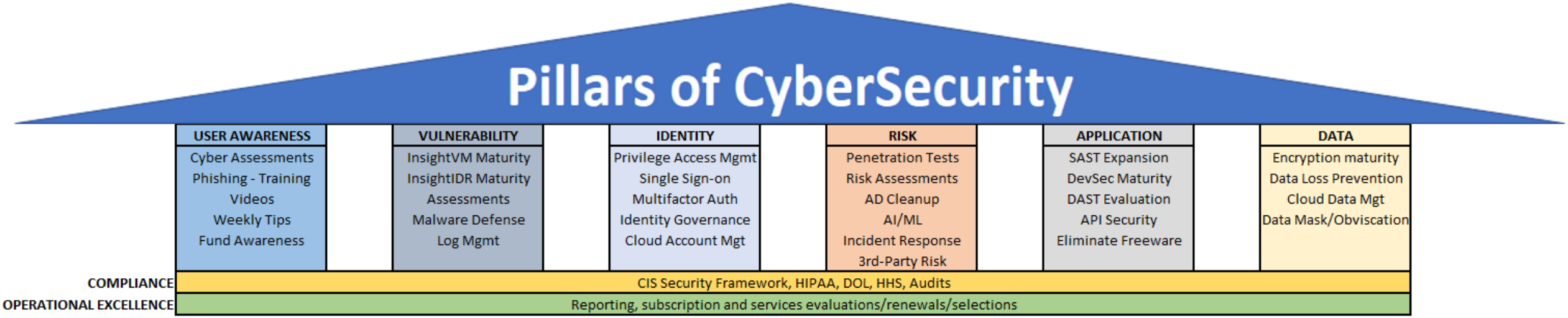
- Email account compromise (phishing, spoofing, hijacking)
  - Continuing compromises seen with several Locals
- 3rd and 4th party risk – the risk introduced by security practices of our partners, their partners, vendors, providers who share or are connected/view/share data
- HHS Breach Report – Ever growing number of breaches (hacks or IT incidents, unauthorized access or disclosures) reported by providers, plans, associates
  - Nearly **500** *reported* breaches of 500+ people in 2024
  - Breaches were reported in all 50 states
  - Nearly **261M** people affected (Change Healthcare 190M, Kaiser 13.5M, Ascension 5.5M)
  - 340M people in US – 261M affected = 77%
  - 120 Summit participants – 77% = 92 people here were likely affected by these breaches last year

U.S. Department of Health & Human Services - Office for Civil Rights

How Do We Protect Your Data?

- **Upgrade, update and patch systems with regularity and urgency – *The #1 issue that organizations have***
  - Workstations, servers, networks, storage, applications
- **Employee awareness and education – *The #2 issue that organizations have***
  - Train on what to look for, what to do, who to contact
  - Identify areas of opportunity to address weaknesses through training
- **Maintain our borders**
  - Firewalls which limit access to our websites, systems and data
  - Geo-fencing – allows access from only approved locations
  - Managed threat detection and response
- **Cyber recovery – prepare for the inevitable**
- **Risk management**
  - Perform external assessments on our environment – penetration testing, audits, remediations
  - Actively monitor and evaluate partner and customer security profiles
- **Identity and Access management and protection**
  - Multi-factor authentication, privileged account management, network segregation

Central States Funds Security Practices



How Does This Help You?

- Foundationally solid security practices help to safeguard your data and maintain our operational stability
- Less downtime on our side = less disruption on your side
- Extension of your teams – we'll share and guide when needed
- Partnerships help us all to be more secure

What Happens If...

- Security Incident Response planning and testing
  - Identify – identify the source of the incident
  - Contain – focus on stopping the threat
  - Eradicate – remove the threat from our environment
  - Restore – restore any compromised systems or data
  - Learn – Post-mortem activities to capture the core issue, what was done to remediate, and what has been implemented to prevent it in the future
- Cyber-recovery solutions – Back up, safeguard and validate data for effective and timely recovery when an event may occur, test frequently to build capability and ensure processes are sound
- Cyber-insurance – Coverage to assist in forensic investigations, assistance to contain and eradicate
- Communication – share appropriate details with the appropriate people at the appropriate time