Preparing Retirement Systems to Manage a Cybersecurity Incident
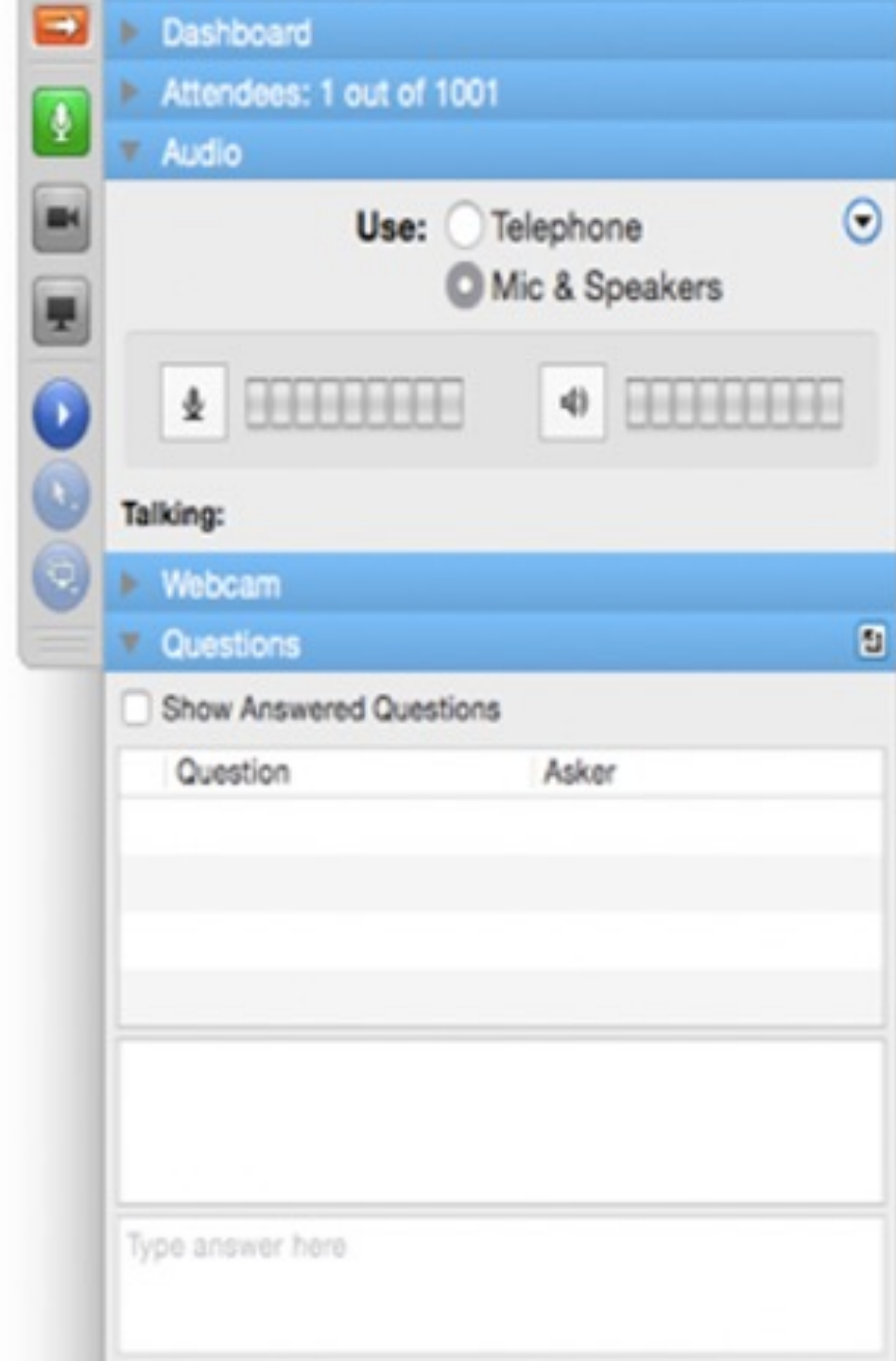
Webinar

October 5, 2022

NATIONAL INSTITUTE ON
Retirement Security
Reliable Research. Sensible Solutions.

Logistics

- Attendees in listen only mode.

- Question are welcome. Submit using "Question" function on control panel

- Audio/technical issues during webinar: call GoToWebinar at 1-800-263-6316

- Webinar replay and slides will be posted at nirsonline.org/events.

Welcome

Dan Doonan

Executive Director
National Institute on Retirement Security

Dan has more than 20 years of experience working on retirement issues from different vantage points including an analyst, consultant, trainer and as a plan trustee. In these various roles, the consistent theme has been his belief that Americans have a shared interest in creating and maintaining a resilient retirement infrastructure that provides adequate financial support in an efficient manner.

Prior to NIRS, he served as a senior pension specialist with the National Education Association. He began his career at the Department of Labor as a mathematical statistician, then spent seven years performing actuarial analysis with Buck Consultants in their retirement practice. His experience also includes positions as a research director and labor economist.

Dan holds a B.S. in Mathematics from Elizabethtown College and is a member of the National Academy of Social Insurance.

Peter Dewar

President
Linea Secure

Peter is a senior strategist with over 25 years of experience in I.T. and cybersecurity. His expertise spans government, energy, not for profit, and health care sectors.

Prior to Linea Secure, Peter spent the last 8 years at the District of Columbia Retirement Board (DCRB), providing strategic technology and cybersecurity direction as CTO and Director of Information Technology. Prior to DCRB, he spent 12 years acting as President of DataFlow Systems, an I.T. consulting firm.

Peter has achieved a Master of Science in Information Systems from The George Washington University and an undergraduate degree in Computer Information and System Science from the University of the District of Columbia. He is a Certified Information Systems Security Professional (CISSP) and has completed the Certificate of Achievement in Public Plan Policy (CAPPP) in Employee Pension.

John Rosenburg, CISM, CRISC, CISSP

Information Security Officer
New York State Teachers' Retirement System

John Rosenburg serves as NYSTRS' information security officer. He directs and manages NYSTRS' information security and risk management programs, and acts in a senior advisory role in decisions affecting information security and assurance. He implements, enhances, monitors and enforces NYSTRS' information security policies and standards. He recommends and approves security policies, standards, processes and education and awareness programs to verify that appropriate safeguards are implemented; and facilitates compliance with those policies, standards and processes. He provides leadership and technical expertise to ensure the integrity, confidentiality, and availability of information assets; oversees and coordinates information security and information assurance efforts across NYSTRS; and exercises enterprise-wide authority for compliance with information security and assurance policies.

Prior to his role as Information Security Officer, John spent thirteen years in various roles within the Information Services department at NYSTRS. Prior to joining NYSTRS, John worked as a consultant for nine years at both Cedar Crestone and William M. Mercer specializing in information systems implementations.

Mr. Rosenburg received his baccalaureate degree in physics from Rensselaer Polytechnic Institute and his master's degree in business administration from the University at Albany. He is a Certified Information Systems Manager (CISM), Certified Information Systems Security Professional (CISSP), and Certified in Risk and Information Systems Control (CRISC).

Jefferey S. Saiger, PMP, CISSP

Chief Technology Officer
State Universities Retirement System of Illinois

Since January 2018, Jefferey has served as the Chief Technology Officer for SURS, where he oversees Information Technology Infrastructure & Operations, Application Development, Project Management, Information Security, Office Support Services and Facilities.

Prior to SURS, Jefferey spent over 20 years working for various enterprise-level organizations across multiple market verticals in leadership roles including Fitch Ratings, General Growth Properties and Tribune Media.

Born and raised in Chicago, Jefferey is a proud Double Demon; holding both a BA (LAS) and MS (IT Project Management) from DePaul University. He also holds several professional certifications including PMP (Project Management Professional) and CISSP (Certified Information Systems Security Professional) accreditations.

Michael Kreps

Principal

Groom Law Group

Michael Kreps is co-chair of Groom's Retirement Services & Fiduciary Group, and he works with a wide variety of clients on complex retirement and health plan issues. His firsthand experience with the legislative and regulatory process gives him a perspective that is often instrumental in helping clients develop and implement effective compliance and advocacy strategies.

Michael advises many of the country's largest benefit plans and service providers on issues related to plan governance, administration, funding, and restructuring.
Michael is an expert on benefit plan recordkeeping and the development of complex financial and insurance products. He also serves as fund counsel to some of the largest benefit plans in the country, including public retirement systems and
VEBAs. Michael helps clients address complex pension funding challenges for both single employer and Taft-Hartley (multiemployer) plans, and he has been involved in over a dozen distress terminations before the Pension Benefit Guaranty Corporation (PBGC).

As a zealous advocate, Michael routinely represents clients before regulators and Congress. He has successfully navigated dozens of Department of Labor (DOL) investigations, including a large number of service provider "book of business" audits. Michael also has secured federal legislation on behalf of clients to, among other things, change the pension funding rules for community newspapers, facilitate retirement plan participation by homecare workers, and provide pension funding relief to a national non-profit.

From the 111th through the 114th Congresses, Michael served as the Senior Pensions and Employment Counsel for the U.S. Senate Committee on Health, Education, Labor, and Pensions. He managed all aspects of the Committee's retirement agenda and had primary staff responsibility for pension legislation, including the pension investment provisions of the Dodd-Frank Wall Street Reform and Consumer Protection Act, the funding stabilization and Pension Benefit Guaranty Corporation reform provisions of the MAP-21 Act of 2012, the Pension Relief Act of 2010, and the CSEC Pension Flexibility Act. He also led the Committee's oversight of regulatory activities involving employee benefit plans.

Michael serves as external general counsel for the Committee on Investment of Employee Benefit Assets (CIEBA) and is on the Executive Committee of the Defined Contribution Institutional Investment Association (DCIIA). He is a graduate of the George Washington University Law School (JD with honors), the University of Colorado (with distinction), and the Sorensen Institute Political Leaders Program. .

Agenda

- Recognizing the Current Threat Landscape

- Preparing an Incident Response Plan

- Steps to Include When Responding to an Incident

- Q & A

Recognizing the Current Threat Landscape

Attack Surface Area will sustain:

- External member self service
- Allowance of remote workers
- Mobile enabled fund managed devices
- Allowance of remote employers
- Allowance of remote 3rd parties
- Increase in cloud application services (I.e., Zoom)

Checkpoint – Has your fund experienced any shifts in cyber posture due to emerging threats?
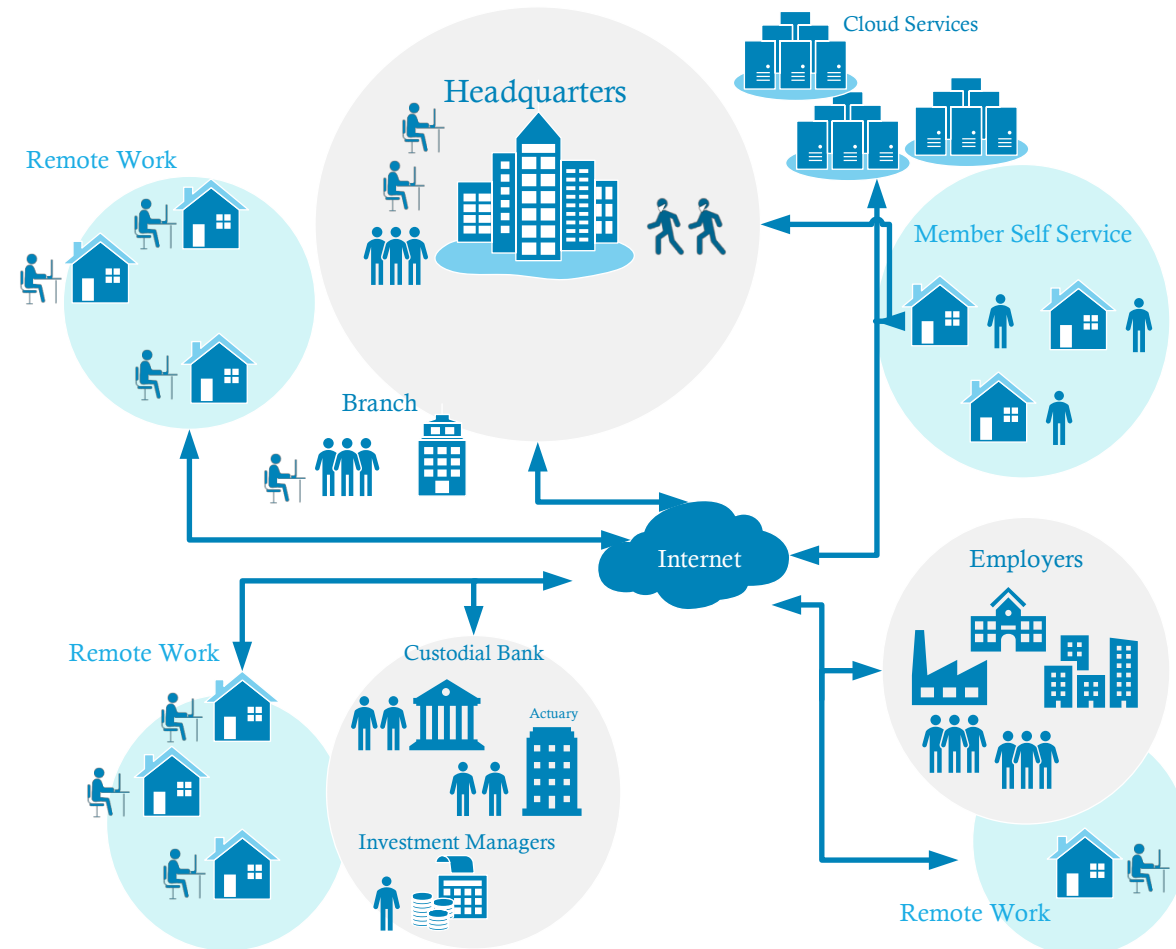
Recognizing the Current Threat Landscape

- Account takeover of member and employer portals

- Data breach

  - Impersonation attacks

  - Ransomware

  - Phishing attacks

- Wire fraud

- Data vendors and other third-parties

Preparing an Incident Response Plan

- Define categories of incidents
- Define roles and responsibilities
- Plan communications
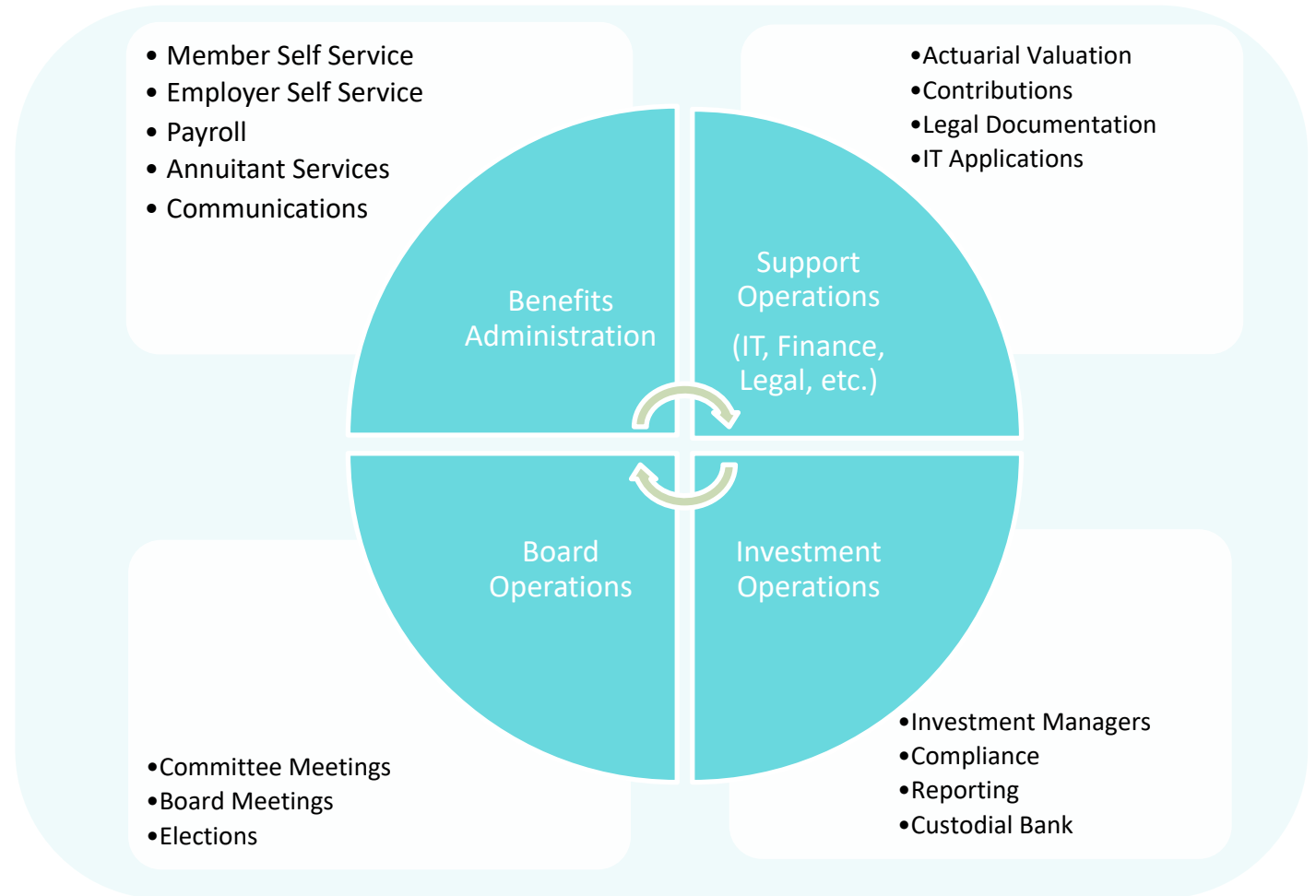- Map out specific steps to resolve each category

Risk transfer (Contracts, Cyber Insurance)

Comprehensive proactive risk assessment

Procedural measures

Technical measures

Evaluating Sources of Cyber Risk

Leverage a holistic view of pension operations to mitigate risk

Checkpoint – Has your fund identified risk in any key business processes?

- Member Self Service
- Employer Self Service
- Payroll
- Annuitant Services
- Communications

- Actuarial Valuation
- Contributions
- Legal Documentation
- IT Applications

Benefits Administration

Support Operations (IT, Finance, Legal, etc.)

Board Operations

Investment Operations

- Committee Meetings
- Board Meetings
- Elections

- Investment Managers
- Compliance
- Reporting
- Custodial Bank

Planning for an event in high risk areas

- Treat cyber risk like organizational risk to get cross-functional buy-in

- Balance likelihood vs impact to focus resources

- Leverage a recognized cyber framework such as NIST cyber polices
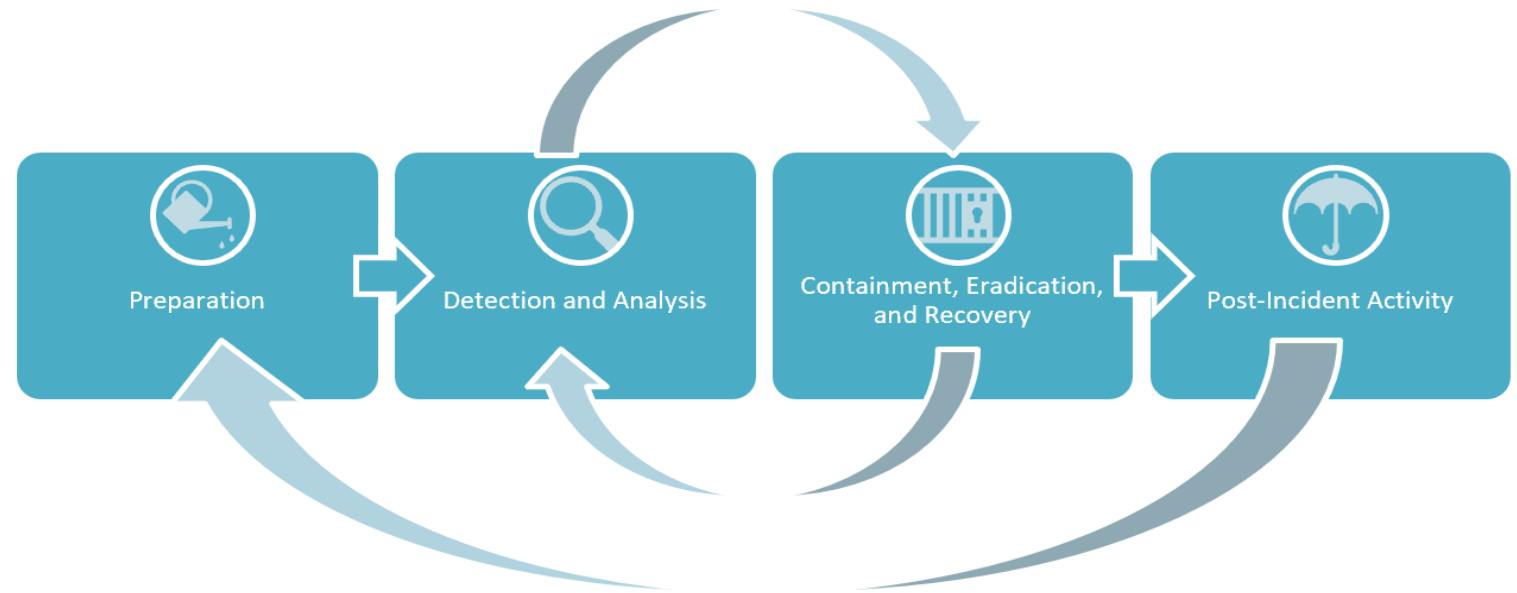
- Tailor the framework to pension operations

RISK MATRIX		RISK IMPACT				
		Low	Moderately Low	Moderate	Moderately High	High
PROBABILITY / LIKLIHOOD	Low				Custodial Bank	
	Moderately Low		Board Communication			
	Moderate				Investment Management	Margin Calls / Payroll
	Moderately High					ESS
	High				Actuary	MSS

Steps to Include When Responding to an Incident

- Engage Counsel
- Utilize cyber insurance and covered services
- Assemble cross functional team
- Root cause analysis

Preparation → Detection and Analysis → Containment, Eradication, and Recovery → Post-Incident Activity

Questions?

Managing Cybersecurity Risks in the Retirement Industry

LINEASECURE

Los Angeles | Washington DC | Toronto