CITY OF Los Angeles
DEFERRED COMPENSATION PLAN (DCP)

# Board Report 19-18

Date: May 21, 2019

To: Board of Deferred Compensation Administration (Board)

From: Staff

Subject: Cybersecurity Review



**Recommendation:**
That the Board (a) receive and file this cybersecurity review for the DCP and (b) refer future study of cybersecurity to the Plan Governance & Administrative Issues Committee for the purpose of (1) developing recommended strategies and structure for addressing cybersecurity risk management and (2) drafting a DCP cybersecurity policy.

Discussion:

## A. Background

At its **December 17, 2017** meeting, the Board's consultants at Segal Consulting (Segal) and its Third-Party Administrator (TPA) service provider, Voya, provided a cybersecurity review for the Board (**Attachment A**). The consultant highlighted fiduciary roles and industry trends and resources. Voya discussed its internal processes, resources, and technology for combatting cybersecurity risks.

On **January 17, 2019**, Segal provided Personnel and City Attorney DCP staff with a pilot cybersecurity workshop (Segal workshop). The Segal workshop is a new educational resource being developed by Segal. The City's DCP was provided the opportunity to participate in the Segal workshop as part of a pilot rollout. The workshop was presented by Jay Preall and Amy Timmons from Segal; Wendy Young-Carter was also in attendance. Unlike a typical cybersecurity training, the Segal workshop concentrated on engaging participants in interactive discussions regarding actual potential cybersecurity events (e.g. data breach or ransomware attacks) targeting the City's operations and functions rather than those of the City's external service providers. The goal of the workshop was to assist staff to assess how communication might unfold, how decisions would be made, how to identify potential gaps in preparedness, and how to produce objectives for improving plans and resources to address an actual event.

At its **February 19, 2019** meeting, staff informed the Board that the training had occurred and indicated that a major takeaway from the training was that cybersecurity risk is broader than cybersecurity risks held with the TPA. Staff indicated that it was conducting a more detailed review of the topic and would provide a fuller report to the Board.

Staff developed the current meeting's report in order to share some of its initial observations and analysis regarding how to approach the challenges posed by cybersecurity risks. However, staff's observation is that cybersecurity is an issue that requires ongoing attention and focus. Consequently, as part of this report, staff has also included recommendations with respect to how to incorporate cybersecurity risk management as an ongoing priority for the DCP.

### B. Approaching Cybersecurity Risk Management

On **October 30, 2013**, Mayor Garcetti issued Executive Directive No. 2 (ED2) requiring that all City departments enhance their own cybersecurity. Each department was given responsibility for securing departmental information and personal user data, overseeing City network usage by its employees and contractors, and ensuring compliance with related Citywide policies established by the Information Technology Agency (ITA).

ED2 created minimum standards that all departments must adhere to including preventing unauthorized access, promoting and enforcing password security, maintaining anti-virus software, promoting a culture of cybersecurity awareness, and planning for business continuity and disaster recovery. ED2 also established requirements for ITA which included creating cybersecurity policies, ensuring departments have proper technology to ensure compliance with ED2, providing software to prompt automatic periodic password updating, and providing annual training for cybersecurity.

ED2 also created the structure for the City's Cybersecurity Organization. The Cybersecurity Organization includes three branches dedicated to making the City's electronic infrastructure more resistant to penetration, able to recover from any disturbance, and able to promote business, innovation, and efficiency (**Attachment B**). The first of these branches is the Cyber Directorate (formerly the Cybersecurity Intrusion Command Center) and is a Mayor-led collaborative effort between all City departments and the Federal Bureau of Investigation (FBI). This working group meets on a quarterly basis to discuss cybersecurity issues and draft cybersecurity policy for the City. Secondly, the Integrated Security Operations Center (ISOC) is the operations branch responsible for implementing enhanced security standards across City departments and serving as a rapid reaction force to cyberattacks. They are located in the City's Emergency Operations Center. The Cyber Lab is a third branch that was recently launched as a public-private-partnership to share the latest cybersecurity threat data, alerts, and intelligence gathered by the City and its partners.

As previously noted, Segal's workshop was focused on internal organizational cybersecurity risk management (rather than risk management for a contracted service provider). The Segal

workshop presenters indicated that there are several types of cybersecurity attacks commonly encountered in day-to-day business and personal activities.

These attacks include ransomware and social engineering attacks such as phishing or email-based traps and scams. Ransomware involves an attempt by an external actor to extort payment in return for stolen data. Social engineering includes a variety of approaches whereby external actors manipulate people into breaking normal security procedures and best practices in order to gain access to systems, networks or confidential information such as usernames and passwords. Cybersecurity weaknesses and exposure can result from unsafe web browsing, weak passwords, and less than optimal approaches to data protection and destruction for both electronic as well as hard copy files.

Following the Segal workshop, staff reviewed a variety of information and held internal discussions as part of developing its own independent construction of how to think about cybersecurity risk management as it applies to the City's DCP. From staff's perspective, the DCP's approach to cybersecurity risk management should best be thought of as existing within a framework that includes both the City's organizational structure as well contracted services. At a high level, the DCP's cybersecurity touch points are illustrated in the chart to the right.


Confidential or important City or participant information is inherent to the administration of the DCP, which exists in the center of the illustration. Exposure risks can exist in any of the systems or processes surrounding the DCP. These include (a) the City's top-level systems (e.g. payroll, email, and web administration systems administered by other City agencies); (b) the Personnel Department's administration of its unique internal systems (e.g. software as well as electronic drives storing data and records generated by its employees); (c) the Employee Benefits Division/DCP staff responsibilities and practices with respect to the receipt, transmission, and storing of confidential data; and (d) the City's TPA/recordkeeper, which stores the vast majority of participant records and data. As an initial step, staff has inventoried, at a high level, cybersecurity risk management resources applying to each of the four core systems/processes surrounding the DCP (**Attachment C**).

Each of these areas requires ongoing attention and, more importantly, *iteration*. The second key observation made by staff following the Segal workshop was that cybersecurity should not be approached simply as a "check the box" list of protective measures which, if implemented,

guarantee protection from all vulnerabilities. The potential vulnerabilities are neither finite nor static. External actors searching for data and financial rewards are constantly evolving their strategies and methods, meaning that organizations must be constantly evolving their defensive methods.

Moreover, anticipating vulnerabilities and creating defenses requires resources, which are not infinite. Each organization must assess and apply its resources prudently, both from a risk management perspective and relative to its other resource demands.

Finally, consideration should also be given to the relationship between cybersecurity risk mitigation and the participant customer experience. Greater protection measures imposed on participants can create frustrations. The DCP should consider whether evolving security requirements imposed on participants are consistent with industry best practices and are adequately communicated to participants so that they understand the basis for change and how to navigate new obligations.

Thus, as the Board, staff, and all DCP organizational stakeholders who are part of managing cybersecurity risk embark more intentionally on the path of cybersecurity risk management, it is important to keep all these considerations in mind. From staff's perspective, it's critical that the topic of cybersecurity risk management receive ongoing attention within an efficient process structure.

For the first phase of its research, certain key findings or actions are summarized as follows:

(1) City of Los Angeles Resources

ITA provides City departments with rapid cyberattack response personnel through the ISOC, systems management resources, software, and support for reporting security issues, and monthly cybersecurity best practice email notifications. ITA also recently issued a Citywide cybersecurity training which will be mandatory for all City employees to complete. This training will support and supplement staff's efforts to manage cybersecurity risks in its internal practices. Additionally, ITA provides a catalog of increasingly sophisticated cybersecurity trainings offered through its vendor Wombat and "table-top" trainings in collaboration with the Mayor's Office and the Cyber Lab. At staff's request, ITA staff is currently coordinating the participation of DCP staff in these upcoming cybersecurity trainings.

Staff has also researched the topic of cyber-liability insurance at the Citywide level. Staff reached out to the City Administrative Officer's Risk Management Division (Risk Management) to inquire about Citywide cyber-liability coverage. Cyber-liability insurance can help mitigate the administrative, technological, and legal costs associated with a data breach. Policies cover a plan's immediate breach costs, which could include credit monitoring, forensic investigations and legally required notification expenses. Risk Management indicates that the City does not currently carry cyber-liability insurance

independent of coverage that is transferred to contractors who house and transfer City data. However, over the last year, Risk Management has been working with the City's insurance broker to package exposure information for submission to insurance markets in order to receive quotes for coverage. Risk Management estimates that this process is nearing its end and that the objective is to create a master policy that covers all City exposures. Staff will continue to monitor this effort.

(2) TPA Resources

As previously indicated, Voya provided the Board with a cybersecurity review in December 2017. Voya is available to provide an updated presentation at any time. Voya has a range of participant-level and recordkeeping-level systems and processes to help prevent and defend against cybersecurity attacks. Voya has provided staff with descriptions of its information security professionals, technology to prevent data corruption and block unknown and unauthorized access to the systems, and policies and supporting controls in place up to or exceeding industry standards. At the participant level, Voya is developing a next-generation website which will include stronger security measures requiring new participants to enter five data points (SSN, ZIP Code, last name, date of birth, and numeric portion of their street address) in order to authenticate their identity when creating their accounts. In addition, the passcode creation protocol will require that a passcode contain between eight and 16 characters. Additional website access protocols will include requiring that participants create a login phrase, select a login image, and choose three security questions with corresponding answers. Participants would be prompted to answer one of the security questions each time they try to access their account via a new device. Furthermore, staff and Voya are presently working on process refinements focused on reducing use of paper forms to reduce exposure to identifying information. It should be noted that the City's contract with Voya includes a data security agreement which codifies Voya's obligations relative to data management and protection, including cyber-liability insurance in the amount of $35 million.

(3) Department and Benefits Division Resources

DCP staff performed an evaluation of the electronic files and reports it currently maintains on the Personnel Department's network server. Staff reviewed these items to gauge whether retaining the files was necessary based on a legal obligation, departmental retention schedule, or operational need. Files that did not meet these criteria were deleted. Moving forward, staff will codify its operational practices with respect to electronic document destruction. This effort is important as it potentially shortens the time needed to re-create priority files, should an intrusion occur. Staff further reviewed hard copy files, reports, and meeting materials in its City Hall office and is in the process of evaluating whether retaining the items is necessary based on a legal obligation, departmental retention schedule, or operational need. Staff reviewed each file type and whether they should be retained in-house, digitized, moved to records retention, or destroyed.

### C. Proposed Structure for Cybersecurity Risk Management and Oversight

In order to develop a sound cybersecurity risk management and oversight structure, staff proposes that the Board refer future study of cybersecurity to the Plan Governance & Administrative Issues Committee for the purpose of (a) developing recommended strategies and structure for addressing cybersecurity risk management and (b) drafting a DCP cybersecurity policy. The Plan Governance Committee, working with staff, can also develop recommendations for the frequency of its and/or the Board's engagement with this topic.

Submitted by: _____
Isaias Cantú

Approved by: _____
Steven Montagna

ATTACHMENT A

# CYBER SECURITY
# What Fiduciaries Need to Know

November 2017

**Wendy Young Carter**
Public Sector DC Director

Segal Consulting

# Fiduciary Role

- A plan trustee is a fiduciary and has the duty to:
  - Protect trust property from loss or damage
  - Preserve the confidentiality and privacy of trust information from disclosure to third party except as required by law or necessary to proper administration
- Selecting a service provider is a fiduciary action
- Trustees have a duty to monitor their service provider

**82%**

**of U.S. citizens are concerned about cybercrime**

Source: Accenture Public Service Citizen Survey, 2017

# What are the Risks?

- The ERISA Advisory Council considers cyber threats a critical risk to employee benefit plans*
- Risks include:
  - Disruption of business operations
  - Reputational harm
  - Participant loss of confidence
  - Potential financial loss for, or impact on, participants
  - Litigation and remediation costs
  - Fines and penalties governments may assess


*See Report on Employee Welfare and Pension Benefit Plans.

# Service Provider Oversight

- Does it have a program?
- Is the program enforced?
- What controls are in place for sensitive data?
- How often does it review and rate its systems for security?
- How does it respond to threats and actual breaches?

# What is a “Cybersecurity Framework”?

- An information security framework is a series of documented processes that are used to define **policies** and **procedures** around the implementation and ongoing management of information security controls in an enterprise environment
- These frameworks are basically a **“blueprint”** for building an information security program to manage risk and reduce vulnerabilities

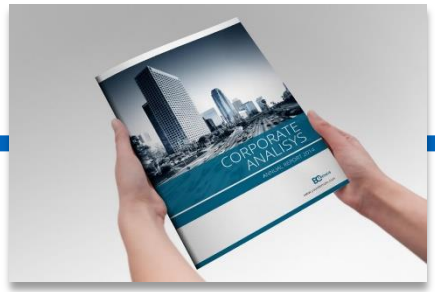



# Industry Developments

- Industry developments include audit standards for defined Ccontribution record keepers' cyber security
- SPARK (Society for Professional Asset-Managers and Recordkeepers) is an inter-industry professional association for financial service companies, investment advisors, third party administrators and benefit consulting firms in the retirement plan industry.

**Record Keeper Hires Third Party Independent Auditor**


**Auditor Uses SPARK's 16 Control Objectives**




**Auditor Creates a SOC2 of AUP Report for Consultants and Plan Sponsors**


**Plan Consultant or Plan Sponsor Uses Report to Grade Record Keepers**

## How It Works

# Thank you!

Segal Consulting

**Wendy Young Carter**
*Public Sector DC Director*
wcarter@segalco.com
202-833-6422

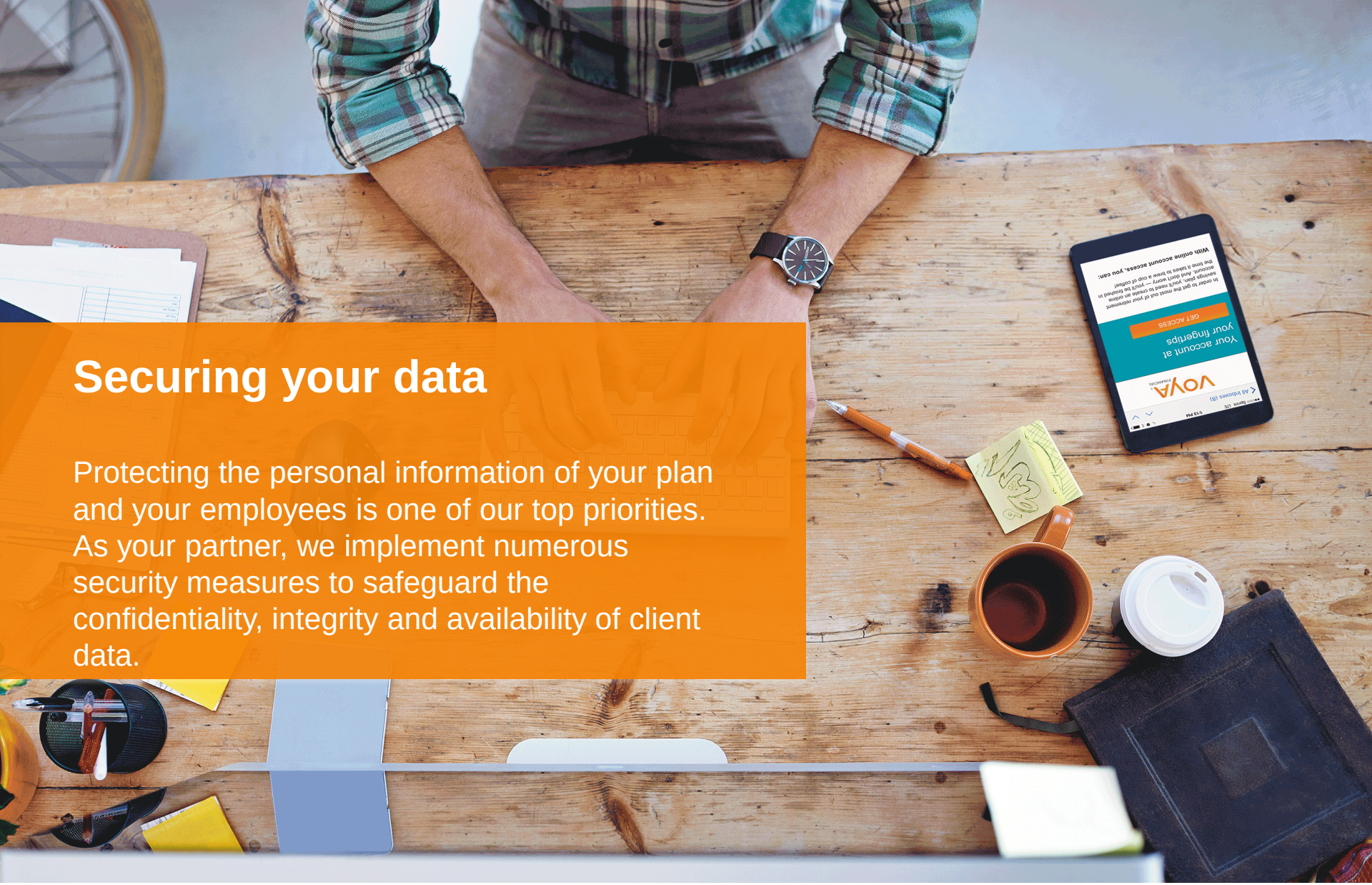
# Cybersecurity Overview

December 5, 2017



PLAN | INVEST | PROTECT

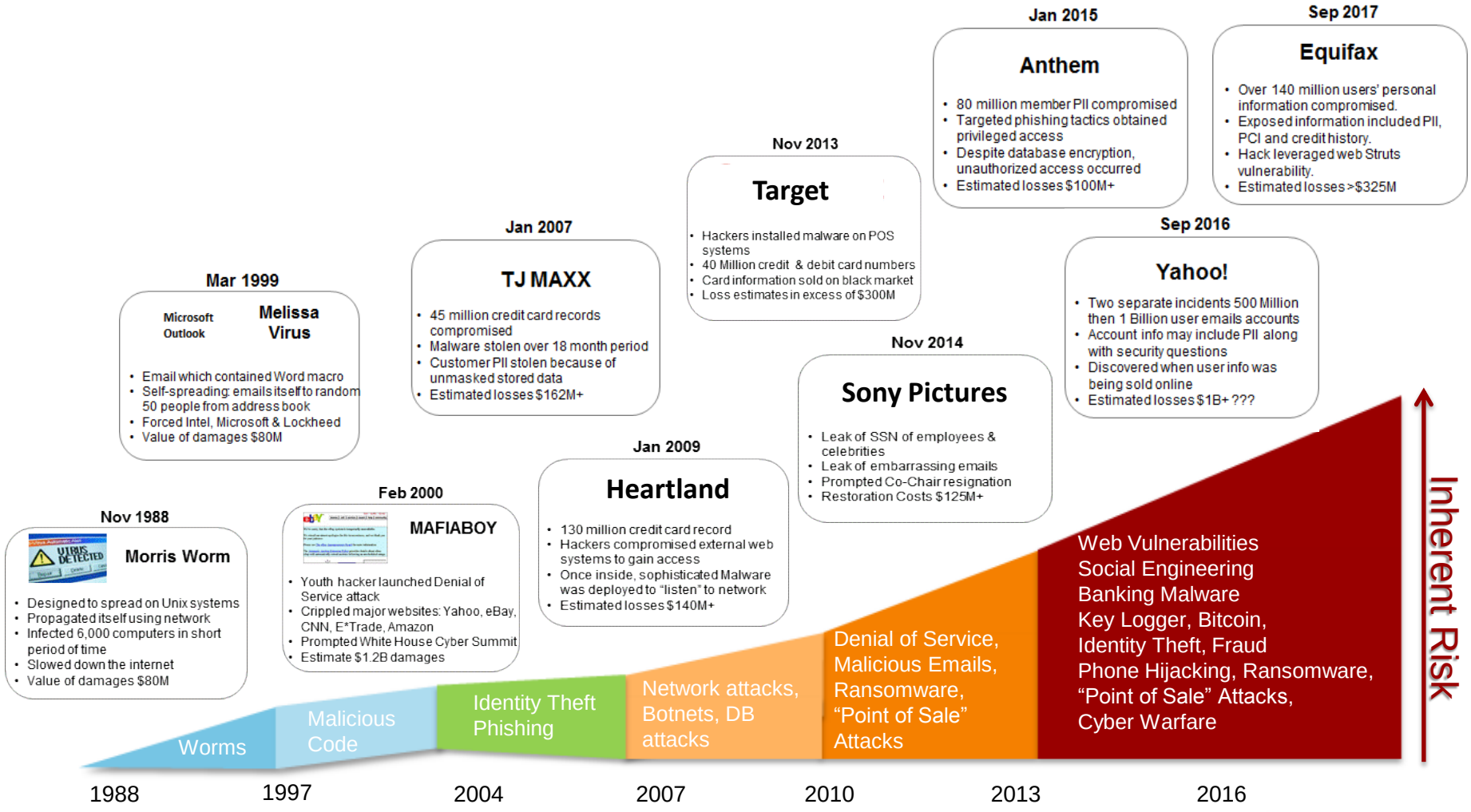
VOYA FINANCIAL




# Securing your data

Protecting the personal information of your plan and your employees is one of our top priorities. As your partner, we implement numerous security measures to safeguard the confidentiality, integrity and availability of client data.

# Evolution of the threat landscape



# People, technology & process to protect client data

**PEOPLE**
Highly skilled security professionals with a robust security awareness program for the entire Voya workforce

**TECHNOLOGY**
Layers of security controls to provide maximum protection with proactive threat intelligence collaboration across the industry, government agencies, and security firms

**PROCESS**
Industry best practice controls and processes to ensure your data is secure

# Our people

## Highly skilled and continuously improving

Conduct monthly phishing tests across Voya Financial™ monthly

**85,000** individual phishing tests annually to train employees on how to avoid phishing attacks.

- Dedicated and certified information security professionals
- Participate in global ethical hacking competitions.
- Trained front line employees as the first line of defense on fraud detection and prevention

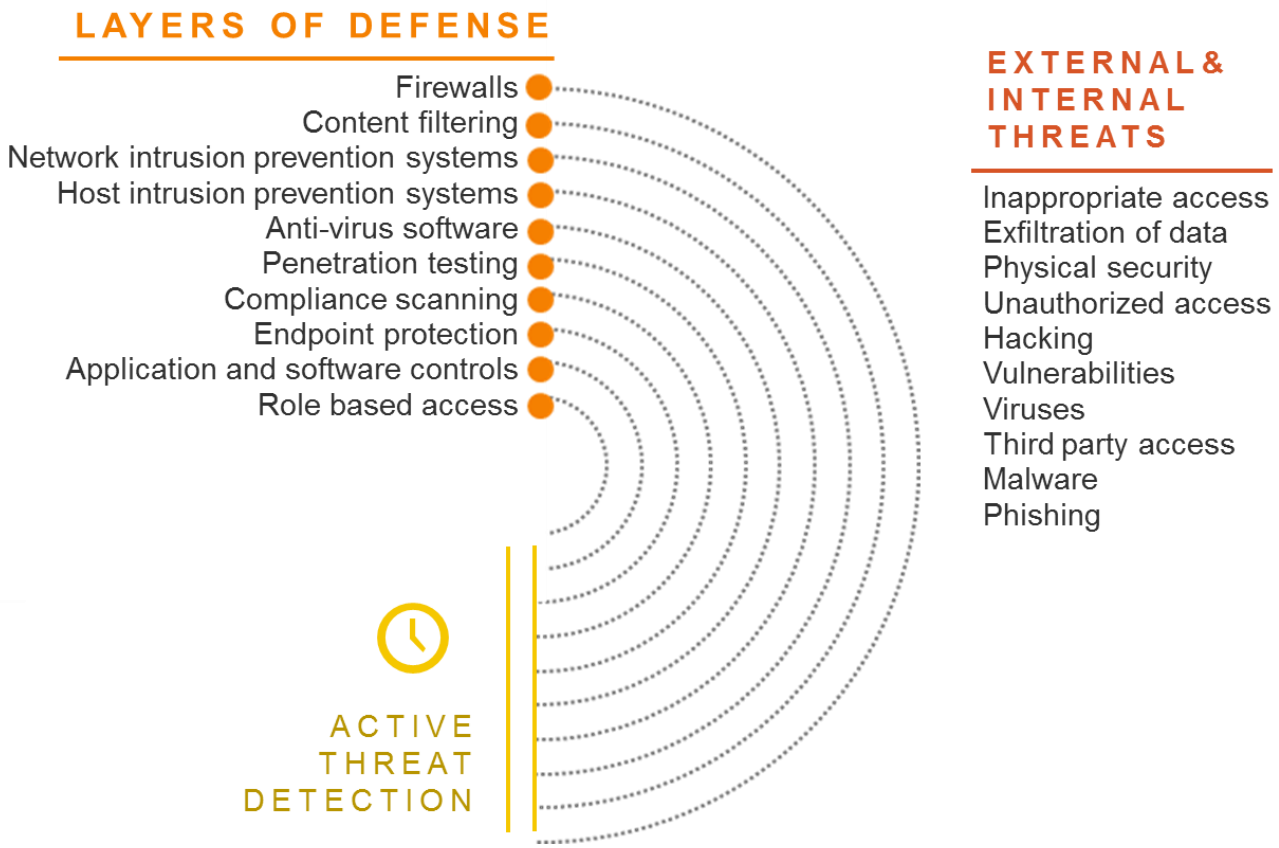
# Our technology

## Protecting your data starts from within


- Automated notification of threat intelligence
- Robust identity verification
- Leverage predictive modeling
- Independent third-party testing

# Our technology - protecting data starts from within

## Designed to prevent corruption of data, block unknown or unauthorized access to our systems and safeguard client data



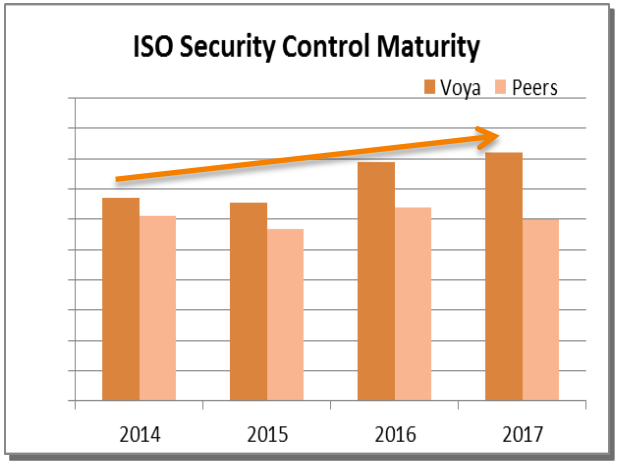
# Our process

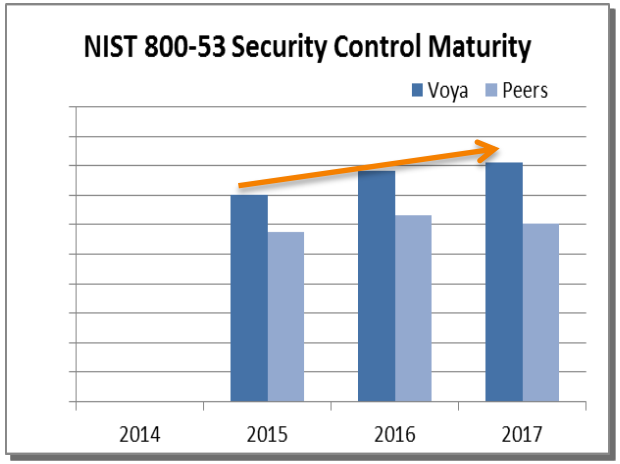
## Industry best practice controls

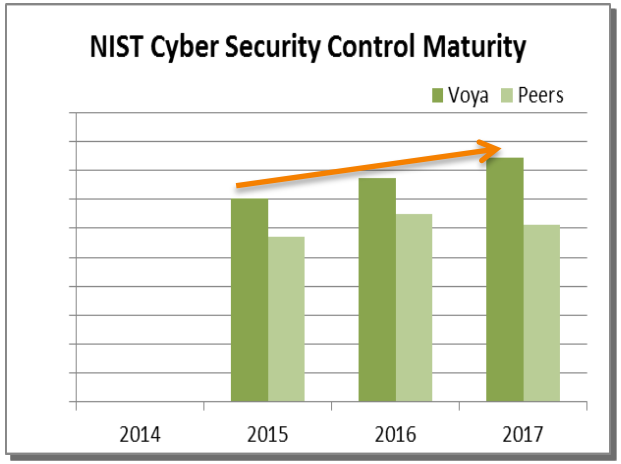
Industry best practice **policies** and **controls** as evidenced by SOC 1 and SOC 2 **certifications**.

- Department of Homeland Security provides us with information on domestic and international threats, which we incorporate into our security protocols.
- Part of a government-sponsored organization that helps us stay informed of security risks
- Compliance to SPARK data security best practice standards
- Peer benchmarking results show that Voya is well aligned and slightly ahead of peers with respect to policies and supporting controls alignment to ISO and NIST standards

# Our Process – Improving Year-Over-Year




Information security management to protect the:

- Confidentiality
- Integrity
- Availability of customer and company information

Security and privacy control requirements for information systems that are used by organizations that support federal entities

Building on the NIST 800.53 standards for:

- Access controls
- Security functions
- Internet security

**Note:** Current CEB/Gartner benchmarks Voya against companies from Financial Services, Insurance, High Tech, Manufacturing, and Retail industries.

# Our process - in the event of a cybersecurity incident

**Voya's highly-specialized security incident response team (SIRT) trained to manage cybersecurity related incidents**

# Q&A

**ATTACHMENT B**

City of Los Angeles
Cyber Directorate

# City of Los Angeles
# Cybersecurity Organization

- ITA Information Security Office
- Mayor's Office of Public Safety

## Strategy & Policy Branch

- **Cyber Directorate** *(formerly CICC)*
  - Executive Body — Mayor – ITA – POLA – LAWA – DWP
  - General Body — ALL DEPARTMENTS
  - Public Safety Body — LAPD – LAFD – EMD
  - State & Federal Liaisons — FBI – DHS – USSS – JRIC – CalOES

## Operations Branch

- **Integrated Security Operations Center (ISOC)**
  - ITA Security Operations Center
  - DWP Security Operations Center
  - LAWA Security Operations Center
  - POLA Security Operations Center

## Partnership Branch

- **Los Angeles Cyber Lab**
  - Public Sector
  - Private Sector
  - DHS SECIR

**ATTACHMENT C**

# Deferred Compensation Administration
# Cybersecurity Resources Inventory

| Tier | Policies / Procedures | Protective Measures | Training & Resources |
|---|---|---|---|
| **Employee Benefits Division** | - Preparing DCP Cybersecurity Policy<br>- Overseeing the Data Security Agreement in Voya contract | - Performing staff assessment of business practices and procedures to identify and address cybersecurity exposures | - Cybersecurity Training (Segal Pilot)<br>- Cybersecurity Training (Annually)<br>- Cybersecurity issue reviews with Board<br>- Coordinating to participate in Advanced Cybersecurity Training provided by ITA consultant (Wombat). |
| **Personnel Department** | - IT Security Procedures Policy<br>- Departmental Records Retention Schedule for Original/Duplicate Records | | |
| **City of Los Angeles Information Technology Agency** | - Executive Directive No. 2 (ED2)<br><br>LINK TO POLICIES:<br>https://www.insidela.org/rules-policies/it-policies/itpc-policies-and-guidelines<br><br>- Internet Acceptable Usage Policy (IAUP)<br>- City of Los Angeles Information Security Policy Manual<br>- Citywide Web Content Policy - Policy # IT-006<br>- Citywide Website Development and Publication Policy - Policy # IT-007<br>- Cloud Services Guidelines Policy - Policy # IT-010<br>- Data Classification<br>- Hardware Refresh - Policy # IT-014<br>- Information Classification Policy - Policy # IT-016<br>- Information Handling Guidelines - Policy # IT-017<br>- Internet Acceptable Usage Policy - Policy # IT-005<br>- IT Disaster Recovery Policy - Policy # IT-018<br>- Mobile Application Development Policy - Policy # IT-008<br>- Password for City's Network and Internet Policy - Policy # IT-004<br>- Password Security Policy - Policy # IT-012<br>- Privacy Policy - Policy # IT-011 | - In collaboration with the Mayor's Office, oversee the convening of the Cyber Directorate, staffing of the Integrated Security Operations Center (ISOC), and Los Angeles Cyber Lab<br>- Oversee the cyberattack reporting system that includes a telephone hotline and email. They are (213) 484-6723 and ita.security@lacity.org<br>- Work with Department of Homeland Security as part of the Multi-State Information Sharing & Analysis Center to share information on cyberthreats<br>- Providing departments with proper technology to ensure compliance with ED2<br>- Providing software to prompt automatic periodic password updating<br>- Providing annual Cybersecurity Training for all City employees | - Cybersecurity Training (Required Annually Citywide)<br>- Monthly cybersecurity best practices emailed to all City employees<br>- Catalog of cybersecurity training modules provided by ITA's vendor Wombat Proofpoint<br><br>https://www.lacyberlab.org/<br><br>LINK FOR RESOURCES BELOW<br>https://www.insidela.org/home/frequently-used-links/cyber-security-awareness-and-training<br><br>ARTICLES<br>- Watch Out for "Social Engineering"<br>-The Growing Threat of "Ransomware"<br>- Myths About Your Computer and Cybersecurity<br>- It's Tax Time ... Don't Become a Victim of Phone Scam<br>- W-2 Information Theft Attempts<br>- How to Spot a Phishing Email<br>- Tips for Safer Online Shopping<br><br>VIDEO<br>- Think Before You Click<br><br>LINKS<br>- Center for Internet Security<br>- SANS.org Ouch!<br>- DHS Cyber Strom - Securing Cyber Space<br>- Federal Virtual Training Environment<br>- ICS-CERT Virtual Learning Portal |

| | | | |
|---|---|---|---|
| **Third-Party Administrator** | | - Over 100 Information Security Professionals performing monthly phishing tests<br>- Technology to prevent data corruption and block unknown and unauthorized access to the systems<br>- Policies and supporting controls in place up to or exceeding industry standards<br>- Multi-factor authentication and identity verification to access website<br>- Timed logoff from the website after an extended period of inactivity<br>- Email encryption to protect personal user information<br>- Firewalls and electronic barriers designed to prevent unauthorized access to the networks<br>- Document control policy that requires sensitive customer information to be locked away when not in use<br>- Employee education and training on TPA's security policies<br>- Collaboration with industry and government intelligence services and cybersecurity firms for comprehensive threat monitoring<br>- Participant education of ways to protect themselves from exposure to | - Cybersecurity Overview Training<br>- Employee Cybersecurity Training |