Seeing the Forest and the Trees
Cybersecurity for Retirement Plans

Presented by:
Carlos González, Attorney, Ogletree Deakins, Atlanta
Stephen Riga, Attorney, Ogletree Deakins, Indianapolis
Jeff Foltz, SVP & Division Manager, Corporate Information Security, Popular
Agenda

• A quick survey of the landscape
• Three common misconceptions
• Cybersecurity in practice
A Quick Survey of the Landscape
Information Held by Retirement Plans
Laws Protecting Personal Information
Recent Litigation Trends
Three Common Misconceptions
Privacy Equals Security
Privacy Equals Security
Privacy Equals Security
Company Security Equals Plan Security
Company Security Equals Plan Security
Company Security Equals Plan Security
A Good Wall Equals Good Security

Good...

...But
A Good Wall Equals Good Security

FACTS
A Good Wall Equals Good Security
Cybersecurity in Practice
Building the Right Team

- Benefits
- HR
- Payroll
- IT
- Legal
Developing a Robust Security Process

• Administrative Safeguards

- Application certification
- Due Diligence & Risk Assessment
- Data Leak
- Phishing Simulations
Developing a Robust Security Process

• Cyber Defense in Depth
Developing a Robust Security Process

• Technical Safeguards

Defense in Depth is designed with the idea to defend a system against any particular attack using several, varying methods. It is a layering tactic, conceived by the National Security Agency (NSA) as a comprehensive approach to information security.

“Defense in Depth” is a military strategy that seeks to delay, rather than prevent, the advance of an attacker by yielding space in order to buy time.

The placement of protection mechanisms, procedures and policies is intended to increase the dependability of an IT system where multiple layers of defense prevent exploits and direct attacks against critical systems.

Goal: Buy the organization time to respond to an attack, thereby reducing and mitigating the impact of a breach.

Slow your click rate on emails – Take time to respond to something that seems “Urgent”....
Developing a Robust Security Process

• Technical Safeguards
Developing a Robust Security Process

• Protection of information

Multi-factor Authentication (MFA)

What are the type of “Factors”

▪ Something you have (ATM Card)
▪ Something you are (Fingerprint, voice, retina scan)
▪ Something you know (Pin, Password)
Sensitive Customer Information is defined as:

▪ A customer’s name, address, or telephone number, in conjunction with the customer’s social security number, driver’s license number, credit or debit card number, or personal identification number or password that would permit access to the customer’s account; or

▪ Any combination of components of customer information that would allow someone to log into or access the customer’s account, such as user name and password or password and account number.

Data Classification Policy link:


Developing a Robust Security Process

• Protection of information

Prevent Identify Theft
Developing a Robust Security Process

• Protection of information

• Mobile devices must be encrypted
• Always keep the laptop with the security padlock. At the end of the functions, keep it in a cabinet with a key
• Never leave the corporate laptop within reach of third parties
• Lock laptops in your car trunk if you must leave your vehicle unattended. Bring devices indoors overnight.
Developing a Robust Security Process

• Protection of information

  Passwords

  ▪ Secret – Don’t share
  ▪ Unique – Don’t reuse
  ▪ Do not save it in the browser
  ▪ Security questions with false answers
  ▪ Multifactor authentication
  ▪ Password management apps
Developing a Robust Security Process

• Protection of information

Password Strength

https://howsecureismypassword.net/

Audit FFIEC

One Hour

23 Seconds

46 Billion Years
Developing a Robust Security Process

• Phishing

Characteristics of the Phishing emails

From: Julio Rivera <jrivera@mackpr.com>
Sent: Monday, November 26, 2018 3:51:05 PM
Subject: MackPR 11/26/2018

See confined proposal for our most recent / upcoming project.
Please bring to my notice if you’ve interest in working on it with us.

My PC won’t allow me send PDF, so I uploaded the proposal document on SharePoint.
Shared folder embedded in

Project#4DC0058.xlsx

Unknown Sender or Known with email compromised
Suspicious Subject
Generic or Missing Salute
Unknown Content
Untrusted Links
Developing a Robust Security Process

• Phishing

Business Email Compromise

Social Engineers:
Physical-Cyber con artists

Exploit the Trust Principle
• Someone you know
• Someone you correspond with often

Risk - Wire Fraud
• Altered Wire Transfer forms or information

Countermeasures
• Verify out of band (Phone call, SMS, Token, etc.)
Developing a Robust Security Process

• Documentation
Developing a Robust Security Process

• Physical Safeguards
Vendors and Contracts

• Services
• Standards
• Monitoring
Seeing the Forest and the Trees
Cybersecurity for Retirement Plans

Presented by:
Carlos González, Attorney, Ogletree Deakins, Atlanta
Stephen Riga, Attorney, Ogletree Deakins, Indianapolis
Jeff Foltz, SVP & Division Manager, Corporate Information Security, Popular