Cyber Security

Working in Partnership to Protect Our Data and Our Participants

Conference Forum 2016

General Board
Pension and Health Benefits
Caring For Those Who Serve

Cyber Security

We're All in This Together!

General Board,
conference and participants—
critical links in a chain
that must not be broken

What's the worry all about?

CREDITS: Writer/Director/Producer: Alex Rosenthal Animator: Nick Hilditch Narrator: George Zaidan

Cyber Attacks—On the Rise*

700 million	Compromised data records in 2014
7 million	Vulnerabilities exploited in 2014—but just **10 accounted for 97% of data security incidents**
99.9%	Of all exploited vulnerabilities occurred more than 1 year after patch was published
$201	Cost per lost record in a data breach in 2014
0.03%	Mobile devices compromised by malware each year • **Beware**—growing threat as organizations embrace Bring Your Own Device (BYOD) programs
23%	Of users fall for phishing—opening e-mails
11%	Of additional users who open unsolicited e-mail attachments

*** Source —Fidelity and Verizon Data Breach Investigations Report**

Most Prominent Methods of Attack*

What is it?

- Via malicious software
- Criminals gain access to private computer systems
  - Gather sensitive personal information (Social Security numbers, account numbers, passwords, etc.)

How do they do it?

Often placed on a computer when unwary user clicks ***unfamiliar link*** or opens ***infected e-mail***

*** Source —Fidelity and Verizon Data Breach Investigations Report**

Most Prominent Methods of Attack*

What is it?

- Via e-mail
- Criminals acquire sensitive personal information

How do they do it?

Masquerading as an entity with which the victim already has a financial relationship (e.g., bank, credit card company, brokerage company or other financial services firm), the criminals solicit ***sensitive personal data*** from unwitting recipients

*** Source —Fidelity and Verizon Data Breach Investigations Report**

Most Prominent Methods of Attack*

What is it?

- Via social media and telephone
- Criminals gain victim's trust over time
- Manipulate victim to divulge confidential information

How do they do it?

Scammers leverage something they know about victim—often from ***social media***—to gain victim's confidence; convince victim to provide more personal information, which can be used to assist in committing fraud

*** Source—Fidelity and Verizon Data Breach Investigations Report**

General Board's Framework of Protection

Customer Protection

Layers of Controls

- People, process, technology

Boundary Defense

- Firewalls, anti-virus, malware protection

Authentication

- Password length, complexity, frequency
- Multifactor

Encryption

- Data and hardware

Patch Management

Rights Management

- Limit access; segregate duties
- Quarterly/annual recertification

Enterprise Risk Management

Cyber Security Insurance

Employee Mandates

- Security Training
- Confidentiality policies

Internal Audit

Mobile Device Management

Security and Fraud Risk Assessments

Third Party Hosting

Validating Results

Annual Vulnerability Assessments

Audits—General Board and critical third parties

- Internal
- External

Application Penetration Testing

Review External Vendor SSAE16

Monthly Internal Network

- Scans, self-assessments

Plan Sponsor and Participant Best Practices

Plan Sponsor Best Practices

Protect yourself, your participants, your organization

- Stay current—operating system (OS) and application **updates**
- Always run commercially sound **security suite**
- Manage **user access and password policies** with robust protection in mind
- Use **encryption** whenever possible—in transmission and at rest
- Practice **robust network management controls**
- Deliver **robust training** to protect your most important asset: your people

Plan Sponsor Best Practices

OS and Application Updates

- **Patching** helps prevent attackers from compromising the system due to vulnerabilities
- If your OS or application can no longer be patched, **consider upgrading to newer version**

Security Suite

- **Use good Anti-X** (malware, spyware, ransomware and virus protection)
  - Reduces likelihood of breaches
  - Better prepares your team to respond to threats

Plan Sponsor Best Practices

Limit Administrator Account Usage

- Including users' accounts with administrative rights

Secure and Protect Disks and Files

- Encrypt drives, if possible
- Store files securely

Plan Sponsor Best Practices—Passwords for Everything

- Work and personal devices
- Websites, applications, confidential files, personal accounts, etc.
- Password recommendations
  - **10+ characters preferred**; 8 characters minimum
  - **Unique** for each account
  - **Not** purely random characters; pneumonic good alternative
  - **Not** common words, birthdays, names of people close to you
  - **Easy for you** to remember; **hard for others** to guess

Password Enforcements

Complexity • History • Change at least every 90 days

Plan Sponsor Best Practices—Password Privacy

NEVER share your username/password

NEVER allow someone to use your username/password

Plan Sponsor Best Practices—Network Management

Never use default passwords

- Protect **edge** of the network
  - Firewalls and/or secured router
- Secure wireless networks
  - Limit access to authorized individuals
- Servers and network equipment—keep in secured, locked room
  - Limit access to individuals with valid need to work with servers/network
- Disable unused services and ports

Plan Sponsor Best Practices—Training

- Invest in ongoing training for your team
  - Good training will likely deliver better return than the latest security software may provide
- Educate users—greatly reduces risk of vulnerabilities caused by operator error

Provide Proper Training for All Staff

- ✓ Good secure practices
- ✓ How to handle certain situations, even on things that seem rudimentary

Examples:

- Remembering to log on and off workstation
- How to use e-mail safely

Other Important Best Practices

- **Assess your environment regularly**
  - Perform health checks/assessments of your environment—from outside and inside
  - Assessments help assure:
    - Doing what is right
    - Nothing is missed
- **Back up data**
  - Develop disaster recovery plan (or at least test backups)
- **Follow policies and procedures**
  - Build documentation as necessary for your organization
  - Require sign-off on training and understanding policies/procedures
- **Follow compliance standards—i.e., HIPAA, PCI, banking regulations**

Do homework before you buy into a cloud application or third-party service

Participant Best Practices

- Manage your devices
- Protect passwords
- Be safe on the Web
- Limit information posted on social networks
- Protect e-mail
- Safeguard financial accounts

Cyber Security

Risk of hack is real!

General Board has received fraudulent requests—e-mails and calls from actors attempting to portray some of you

Our controls detected and prevented these attempts

We must be in partnership—protecting our data!

General Board

Pension and Health Benefits

Wespath

Investment Management