Risk Management for Trustees: Cyber Liability Insurance and Identity Theft Protection

Presented by Arthur J. Gallagher & Co. and Ullico Casualty Group Inc.
Cyber Liability Insurance:
Protection for benefit funds

Brandon Cole
Area Vice President
Arthur J. Gallagher & Co.

Tina Fletcher
Vice President
Ullico Casualty Group Inc.

Arthur J. Gallagher & Co.
BUSINESS WITHOUT BARRIERS™

Ullico
What is a Data Breach?

• Data Breach: is an incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorized to do so.

• Identity Theft occurs after a Data Breach and criminals use stolen data to make purchases, apply for loans, withdraw money or commit fraud.

• Who should be concerned about data breaches?
  – Personal Identifiable Information (PII)
    • Social Security #s
    • Dates of Birth
    • Addresses
    • Bank Account Information
    • Health Care Information
  – Other information that can be breached:
    • Credit/Debit Card Numbers
    • Emails, Password and User Names

• Cyber breaches are regulated by the States, exceptions:
  – Health care breaches are reported to HHS
  – 12 states have started reporting breaches
Data Breaches – NOT IF BUT WHEN!

• Data Breaches tracked at the Federal level; Up by 40% in 2016:
  – Hacking, Phishing Scams, and Skimming are on the raise (55.5% of the attacks in 2016, up by 17.7% since 2016; Impacted over 26M records from 607 reported breaches)
  – Accidental Email/Internet Exposure (9.2% of breaches)
  – Employee Error, Negligence, Improper Disposal, Loss of Data
  – Insider Theft, Physical Theft
  – Subcontractor, 3rd Party or Business Associate
  – Data on the Move

• 52% of breaches involved Social Security #s
• 8% involved Credit Card numbers
• 40% involved other PII
• Causes
  – 42% are intentional
  – 30% caused by human error
  – 28% system glitches and vulnerabilities

Data Breach Examples – Public Funds and Unions

- Union accidentally printed social security numbers in the address label of marketing brochures that were sent to members.
- Employee of a public pension fund posted an unencrypted file on a public website, compromising personal information for over 2,000 members.
- Retirement system inadvertently placed pension participants personal information on a server that was open to the public.
- State retirement system sent unencrypted computer discs with personal information for over 44,000 members to the health office; spent over $300,000 just to ensure that the information was not obtained by unauthorized users or that the information was not misused in any way.
- Hackers stole personal data for over a million Japanese citizens from the country’s pension system.
- Police Pension system lost $130,000 as a result of two unauthorized wire transfers.
- Scammers got access to retirement accounts and took fraudulent loans worth $2.6 million.
- Police Pension system realized that hackers compromised over 300 officers’ personal information.
- Phishing attack compromises school district employee data.
- 3,000 community college workers victimized in W-2 scam.
But we have IMMUNITY, right?

• Risk Exists:
  – Most states have passed laws that apply to public agencies
    • 30 day notification requirements
  – If your state grants immunity you may still have obligations:
    • Immunity doesn’t always extend if participants reside in other states/countries
    • Public Relations Nightmare – reputational impact
    • Internal Nightmares – financial impact, administrative impact (time and money)
    • Federal Laws apply, such as HIPAA and FERPA
  – Questions to discuss with your plan sponsor/municipalities and your colleagues:
    • Do you have protection if you are found personally liable
    • Who is responsible for notifications
    • Who is responsible for speaking with the press
    • Do we have someone with expertise in cyber laws across the country (not all retirees live in your state or jurisdiction)
Cyber Insurance

- Risk Transfer
  - Prices are very reasonable
  - Not all policies are created equal
  - Negotiated partnerships with privacy counsel and incident response vendors = more value for your dollar and quick response time

- Coverages
  - Privacy liability
  - Breach notifications
  - Media liability
  - System damage & business interruption
  - Regulatory proceedings
  - Threats & extortion
  - PCI fines
Cyber Insurance

- Risk Management Tool
  - Expert resources help insure compliance, protects reputation (many policies include PR coverage), and ensures operational efficiencies
  - Hotline to call when a breach occurs – before the claim is even reported
  - Provides credit monitoring to try and help mitigate future liability

- Overlap in coverage with other policies
  - Fiduciary Liability policies – unless there is a cyber exclusion
    - Penalties
    - Breach of Fiduciary Duty
    - Vendor Selection
    - Some carriers provide optional cyber coverages but not as broad

- Not Covered
  - Review Exclusions
  - Most policies do not cover telecommunication risks
  - Theft of Assets
    - Bonds cover theft
Safety Tips and Risk Management

• The only safe computer data system that is truly secure is one which is switched off and unplugged!

• Cyber Breach Procedure should be in place
  – Fiduciary responsibility to protect your participants’ data
  – Make sure the policy is being followed
  – Address participant negligence within the policy
  – Address thefts and portable equipment
  – Establish a response czar who will lead if a breach occurs

• Other policies
  – Breach response plan
  – Social media/external postings/blogs/instant messaging
  – Website content
  – Personal devices
  – Medical privacy

• Create a culture of data privacy awareness
  – It all starts with individuals that handle the PII – employees and vendors
  – Educate on incident reporting procedures and phishing schemes
  – Educate retirees

• Contractors and Consultants
  – Centralize agreements
  – Indemnification language
  – Do your vendors have cyber breach policies in place
  – Do your vendors have cyber insurance
Safety Tips and Risk Management

- Other Tips:
  - Limit employee access to sensitive information
  - Conduct regular audits
  - Use antivirus software
  - Insert firewalls, pop up blockers
  - Uninstall any unnecessary software
  - Maintain backup information (run daily at a minimum)
  - Check security settings
  - Use secure connections
  - Use Encryption
  - Setup a multi-factor authentication for participants to access records
  - Require participants to create strong passwords and require they change it regularly
  - Be prepared for the Worst!
Tips for Individual Users

• Limited protection, if any, when consumers are responsible for sharing their own PII
  – Don’t use public wi-fi services, work computers, or public computers to check your accounts
  – Be cautious when using unfamiliar ATM machines and credit card scanners
  – Use caution before clicking on links or opening attachments
  – Do not reply to emails or inbound phone calls that ask for account or personal information
  – Monitor your account statement, checking balances, transaction activity – every month!
  – Create strong passwords, security questions and change your password frequently
  – Don’t share passwords with anyone
  – Check your credit report regularly
Reporting Cyber Crimes

- Determine state requirements for reporting cyber crimes
- Reporting cyber crimes to other governmental authorities:
  - United States Department of Health and Human Services
    - [https://www.hhs.gov/](https://www.hhs.gov/)
  - Econsumer.gov
  - The Department of Justice (DOJ)
  - Federal Bureau of Investigation Internet Crime Complaint Center (IC3)
    - [https://www.ic3.gov/complaint/default.aspx](https://www.ic3.gov/complaint/default.aspx)
“The database compromises of 2016 confirmed yet again that breaches are the 3rd certainty in life and we are all living in a constant state of cyber insecurity”

~ Adam Levin, Chairman of CyberScout
Identity Theft Protection:
Critical Benefit for Public Employees

Don Heilman
Area Senior Vice President
Arthur J Gallagher & Co.

Gallagher Benefit Services, Inc.
2016 Data Breach Hacking / Skimming / Phishing

Top categories - number of records exposed:

1. Healthcare…**12,919,028**…35%
2. Government & military…**7,438,407** or 24%
3. Business…**5,463,150** or 15%

Banking, credit & financial no longer the leading category

Source: ITRC
And That is Only Half the Picture…

- Of the 1,039 breaches, only 539 are used to tally the total number of records compromised. The other 554 breaches are considered “unknown” and therefore not counted in number records compromised.*
- Many incidents involving only emails, user names, and/or passwords are not included in the overall total number of records compromised.**
- Currently, state laws specify the types of personal information that must be breached in order to require an institution to notify affected consumers.**
- Generally, the law will require official notification only in the case that PII is compromised in combination with the consumer’s full name.**
- Generally, online user names and passwords for financial accounts can be used without the consumer’s name to gain account access.
- Many of the large breaches which compromised hundreds of millions of user names and passwords may not have had a legal obligation to notify customers quickly, i.e. Yahoo, LinkedIn, etc.
- Retirement and pension accounts could be accessed and funds siphoned off fraudulently by simply using the account credentials stolen in a breach event months or even years before.

Sources: *ITRC **2014 Javelin Study
• 150 million Social Security numbers were exposed in breaches in 2015
• 43% of survey respondents reported that their stolen information was used to file tax returns in their names, get drivers’ licenses, or obtain jobs, up from 32% in 2014
• Criminal identity theft - even more devastating
• Of the 20% of respondents who experienced criminal identity theft, more than 60% had to borrow money
• Nearly 33% used savings to pay for expenses
• 44% lost a job opportunity
• 31% lost their place of residence
• 33% could not qualify for a home loan
• Nearly half had to rely on friends and family for assistance
• 56% missed time from work

Source: Aftermath Study by Identity Theft Resource Center
Experian’s 2016 Data Breach Forecast

- New payment technologies are not a panacea for payment breaches and fraud
- e-commerce sites for retailers - next wave of attacks?
- The U.S. Director of National Intelligence - cybercrime #1 national security threat, ahead of terrorism, espionage and weapons of mass destruction
- Likely to see more incidents aimed at stealing corporate and government secrets or disrupting military operations.
- Possible increase in large public sector data breaches (remember the 2015 Office of Personnel Management breach?)
- Hacktivism will make a comeback…cyber criminals - not motivated by financial gain
Early Warning and Detection is Critical

- 35% of employers have added identity theft protection as a voluntary benefit - projected to double by 2018
- A basic program provided on an employer paid basis - less than $36 per year
  – With no taxable consequence to employee
- Buy-up options typically offered for higher levels of coverage, including dependents

* Willis Towers Watson 2016 VBS Survey
Features to Look for in Identity Theft Protection Program

- At or near real-time alerts
- Real insurance vs. service guarantee
- Fraudulent loss of funds coverage up to the full face amount of policy
- Extensive black market monitoring of PII (personally identifiable information)
- Qualified recovery specialists
Desirable Additional Features

• 3 bureau monitoring and alerts at or near real-time
• 1 or 3 bureau report & score, with monthly or quarterly updates (annual update not sufficient)
• Deep monitoring and alerts of financial and personal information activity
• PC keyboard encryption software
• Family coverage options
Provider Considerations

• **Proven** data security through regular audit
• Compliance…built into system
• Transparency in marketing practices
• Direct relationships with credit bureaus and data providers vs. buying components and bundling
Thank You