NWCM

VOYA FINANCIAL

Cybersecurity Threats: Insights and Strategies to Help Protect Your Retirement Plan

SCOTT T FISHER, CFA

NORTHWEST CAPITAL MANAGEMENT INC.

VP ADVISORY SERVICES

CHARLES GRIFFIN, CISSP

TECHNOLOGY RISK & SECURITY MANAGEMENT, VOYA FINANCIAL™

IT SECURITY CONSULTANT

Agenda

- The Legal Landscape
- DOL Cybersecurity Guidance
- Cybersecurity Best Practices
- Resources for Plan Sponsors
- Key Recommendations
- Questions & Answers

The Legal Landscape

RECENT CASES

A number of lawsuits have been filed concerning data security lapses that have resulted in money lost from retirement accounts

1. ***Bartnett*** a participant is alleging that the plan fiduciaries failed in their duty to exercise appropriate care in hiring their recordkeeper. (Loss was $245,000. Claim has been dismissed twice, but may still proceed if she can show fiduciaries acted in a manner that was 'objectively unreasonable.')

2. ***Prior case in 2015*** $400,000 was stolen from a 401(k) account through the use of fraudulent forms.

3. ***Additional recent report*** $99,000 theft of plan assets.

DOL CYBERSECURITY GUIDANCE

In April, the DOL issued three pieces of guidance addressing the cybersecurity practices of retirement plan sponsors, their service providers, and plan participants:

1. ***Tips for Hiring a Service Provider*** outlines factors for business owners and fiduciaries to consider when selecting retirement plan service providers.

2. ***Cybersecurity Best Practices*** is a collection of best practices for recordkeepers and other service providers, which may be viewed as a reference for plan fiduciaries when evaluating service providers' cybersecurity practices.

3. ***Online Security Tips*** contains online security advice for plan participants and beneficiaries.

TIPS FOR HIRING A SERVICE PROVIDER

1. Ask about the service provider's data security standards, practices, policies, and audit results and benchmark those against industry standards.

2. Analyze the service provider's security standards and security validation practices.

3. Evaluate the service provider's track record in the industry.

4. Ask about past security events and responses.

5. Confirm that the service provider has adequate insurance coverage for losses relating to cybersecurity and identity theft events.

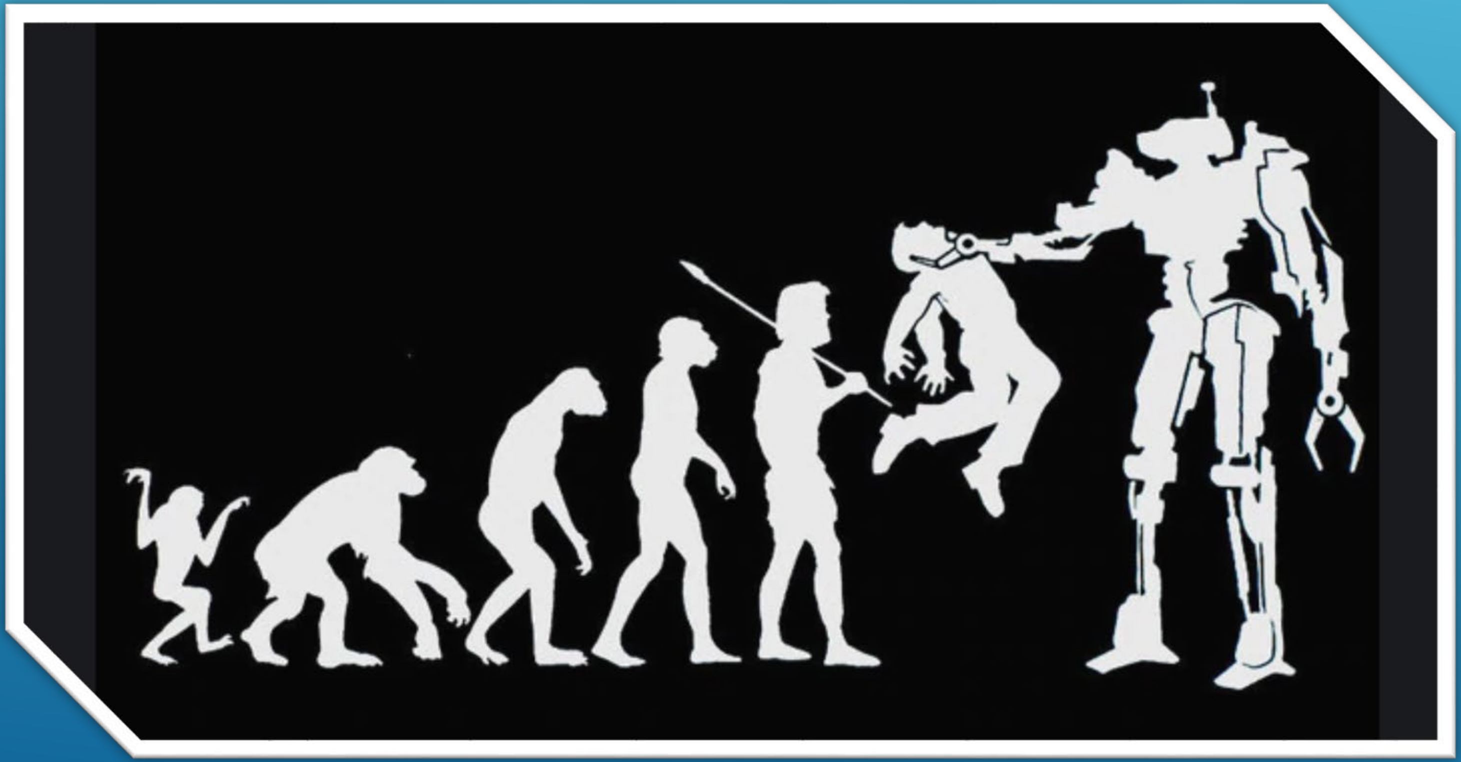
6. Ensure that the services agreement between the plan fiduciary and the service provider includes provisions requiring ongoing compliance with cybersecurity standards.

CYBERSECURITY BEST PRACTICES

1. Have a formal well-documented cybersecurity program.
2. Conduct prudent annual risk assessments.
3. Have a reliable annual third-party audit of security controls.
4. Clearly define and assign information security roles and responsibilities.
5. Have strong access-control procedures
6. Ensure that any assets or data stored in a cloud or managed by a third party are subject to appropriate safeguards.
7. Conduct periodic cybersecurity training.
8. Implement and manage an SDLC (software development life cycle) program.
9. Have an effective business resiliency program addressing BCDR (Business continuity and disaster recovery) and incident response.
10. Encrypt sensitive data, stored and in transit.
11. Implement strong technical controls in accordance with best practices.
12. Appropriately respond to any past cybersecurity incidents.

CYBERSECURITY BEST PRACTICES

… or how to control your technology and not be a victim of it!



CYBERSECURITY BEST PRACTICEs

Employee = phishing, surfing

Create passphrases – not passwords

Don’t share user names or passphrases

NEVER use your SSN or DOB – EVER!*

https://haveibeenowned.com/

…try it …

*There are more tips for participants in the Appendix

PLAN SPONSOR RESOURCES

https://www.nist.gov/
The National Institute of Standards and Technology's Cybersecurity Framework is a set of guidelines for private sector companies to follow to be better prepared in identifying, detecting, and responding to cyber-attacks.

https://www.sans.org/
The SANS Institute is a trusted resource for cybersecurity training, certifications and research.

https://www.iso.org/isoiec-27001-information-security.html
The International Organization for Standardization (ISO)'s standards for information security.

https://www.isaca.org/resources
ISACA (the Information Systems Audit and Control Association) offers a variety of training options from knowledge-based to practical training and credentialing.

https://www.educause.edu/
Through the EDUCAUSE Cybersecurity Program, you can find the tools, resources, and peer connections

https://www.sparkinstitute.org/
Free resources to help plan sponsors reduce exposure to various threats, learn about industry best practices, and get information about how to respond in the event of an incident.

https://www.coso.org/Pages/default.aspx
An initiative dedicated to helping organizations improve performance by developing thought leadership that enhances internal control, risk management, governance and fraud deterrence.

https://www.dol.gov/general/topic/health-plans/fiduciaryresp
Important information about fiduciary responsibilities for plan sponsors.

https://www.sba.gov/content/introduction-cybersecurity
Small Business Cybersecurity resources, information & tools.

https://www.ftc.gov/tips-advice/business-center/small-businesses
Cybersecurity tips, advice, and resources for businesses

https://cyberreadinessinstitute.org/starter-kit/
The Cyber Readiness Starter Kit is a free, fast way for small businesses to provide employee cybersecurity awareness training on cyber issues.

https://nationalcybersecuritysociety.org/small-business/resources/
Recommended cyber best practices and educational products developed with small businesses in mind.

https://www.dfs.ny.gov/consumers/small_businesses/cybersecurity
Cybersecurity tools for small businesses from the Department of Financial Services (DFS).

PLAN SPONSOR RESOURCES – AND CURRENT EVENTS

Business Next-Generation Firewall (NGFW)
(Your door to the Internet)

SonicWALL
Fortinet
Palo Alto

Frequent automatic threat signature feed updates

Recent Events of Note

1. Colonial Pipeline
2. Transamerica
3. Abbott Labs

KEY RECOMMENDATIONS

Plan Fiduciaries Should Consider the Following:

1. Involve Enterprise IT or outside support
2. Draft a plan to respond to the new standard
3. Document efforts, discussions, planned action steps
4. Utilize resources as necessary
   1) Involve service provider in training and support
   2) Utilize plan counsel for advice and agreement review

Questions & Answers

Thank You

Scott T Fisher, CFA
Northwest Capital Management Inc.
Phone: 206.707.7596 | Email: scottf@nwcm.com

Scott is Vice President of Advisory Services with NWCM and is an expert in the retirement plan space, holding the Chartered Financial Analyst (CFA) designation. Scott provides plan fiduciaries with investment counsel aimed at allowing them to make plan stewardship decisions with high confidence.

Charles Griffin, CISSP
Voya Financial™

Charles Griffin, CISSP 50745, started his career in cybersecurity in 2000 as a Network Consultant. At Voya - he is sharing with plan sponsors, consultants and advisors – the nearly two-decades of experiences with cyber threats and security measures of which he has had first-hand experience.

Appendix

ONLINE SECURITY TIPS

Nine Tips for Participants:

1. Register, set up, and routinely monitor account
2. Use strong and unique passwords
3. Use multifactor authentication
4. Keep personal information current
5. Close or delete unused accounts
6. Be wary of free Wi-Fi
7. Beware of phishing attacks
8. Use antivirus software and keep apps and software current
9. Know how to report ID theft/incidents

Administrator Considerations

Encouraging participants and beneficiaries to follow these tips to reduce risk and help mitigate exposure to cybersecurity threats

CYBERSECURITY BEST PRACTICES

Apply software updates to servers and systems

Don’t allow browsers or social media sites to memorize your passphrase

Open your financial statements and review to verify all activity on your account

Make sure your all your systems have a firewall (and it is working)

Windows Defender Firewall or equivalent

CYBERSECURITY BEST PRACTICES

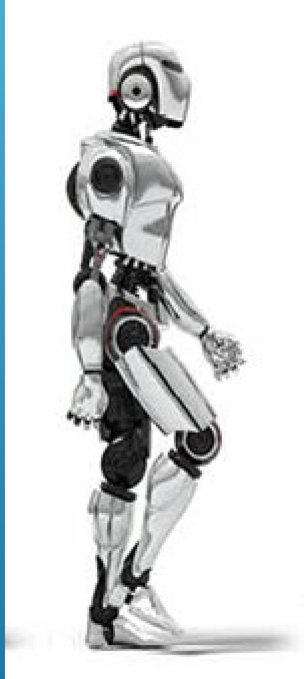
Register your account if asked to by your bank, employer etc.

Check your account at least quarterly

Use two-factor authentication

DON'T OPEN emails if you don't know the person or source

CYBERSECURITY BEST PRACTICES



Check your credit report
https://www.annualcreditreport.com/index.action

Check to see if your email has been compromised
https://haveibeenpwned.com/

Use Firefox browser (more secure)
https://www.mozilla.org/en-US/firefox/browsers/

Use a privacy search engine
https://duckduckgo.com/

If you become a victim of ID theft:
https://identitytheft.gov/

CYBERSECURITY “REALLY” BEST PRACTICES

Use one dedicated system for
all on-line financial transactions – NO SURFING

Purchase and use a VPN – Nord, ExpressVPN, etc.

Public Wi-Fi (Avoid) – use your cellphone as an access point

Turn-off Bluetooth when not using

Never use “public” USB charging ports