2022 Cybersecurity: best practices overview

Agenda topics

- Global trends in cybersecurity – what we are seeing
- DOL's cybersecurity best practices: How Empower meets and exceeds the DOL guidelines (ask your Relationship Manager for our response to these guidelines)
- Ways Empower is protecting data
- What we can all do to improve data security
- Q&A

Global trends, threats and vulnerability statistics

- 70% of ransomware attacks include data exfiltration (usernames & passwords)[+]
- 3 Most common compromise points for ransomware: phishing, unpatched exploitable vulnerabilities, remote desktop protocol (RDP sessions)[++]
- CVE global annual vulnerability stats: 2020 had 28,000 new vulnerabilities. 2021 had 45,000 new vulnerabilities.
- Global records stolen (per billion): 19 billion records stolen in the first half of 2021.[*] 2020 had 27 billion records stolen in the top 10 breeches alone.[**]

What are the bad actors up to?

Phishing through email: #1 successful attack platform for bad actors[1]

Organized Crime is trending up (targeting CARES Act, Unemployment Insurance, Social Security Administration, Paycheck Protection Program)[2]

"**Families behaving badly**" is trending up[2]

2022 FBI PSA: Cybercriminals tampering with QR Codes to steal victim funds[3]

Ransomware grew 1070% year over year[4]

Smishing (SMS/Text message Phishing) attempts are increasing[5]

Increasing ransomware-as-a-Service: Cybercriminals acting like capital investors, funding startup cyber-criminal organizations such as Darkside Ransomware[6]

Shortened URL links are now used as Phishing hooks[7]

Please note the difference between breach and fraud.

Empower has not experienced a security breach of our systems. If a threat actor attempts to access a participant account, Empower has a multilayer fraud control environment to protect your assets and data.

[+] Health IT Security, Phishing Top Entry Point, February 2021

[++] xorlab, Most Common Ransomware Attack Vectors, February 2022

[*] Biggest breaches of 2021, Security Boulevard, December 13, 2021

[**] Biggest breaches of 2020, Security Boulevard

[1] 2021 Verizon DBIR Figure 20 Top Action varieties in breaches

[2] Empower Proprietary Research 2021

[3] FBI Public Service Announcement, January 2022

[4] Fortinet "FortiGuard Labs Global Threat Landscape report"

[5] ITPro "Smishing attacks increase 700% in first six months of 2021"

[6] TechTarget "Darkside Ransomware funded by cybercriminal 'investors'", June 2021

[7] 2021 Proofpoint "State of the Phish – Annual report"

FOR FINANCIAL PROFESSIONAL USE ONLY.

DOL's cybersecurity best practices: Learn how Empower meets and exceeds these guidelines as evidenced in these documents.

- 12 Cybersecurity program best practices for recordkeepers and service providers
- 6 Tips for plan sponsors
- 9 Online security tips

Please ask your Relationship Manager for more information on Empower's response to the DOL guidelines.

Ways Empower is protecting data

For our plan sponsor clients:

- Modern platform
- Annual SOC 2 type 2 reports
- Third-party validation
- Quarterly risk assessments
- Penetration testing
- Dark web monitoring
- Fraud prevention
- Cloud technology
- Ongoing disaster recovery exercises

For our participants:

- We encrypt your data
- We don't sell your data
- We partner with cybersecurity leaders to keep your information safe.
- What happens if I have ID theft or email compromise? We have your back.
- Did you know Empower has a Security Guarantee?

Our Security Guarantee

We will restore losses from your participants' accounts that occur as a result of unauthorized transactions that occur through no fault of their own.

SECURITY GUARANTEE

Reimbursements associated with the Security Guarantee are subject to certain conditions set forth at participant. empowerretirement.com/participant/#/articles/securityguarantee

FOR FINANCIAL PROFESSIONAL USE ONLY.

Empower cybersecurity best practices: What we can all do to improve data security

5 best practices for plan sponsors to increase plan security

1. Provide accurate, up-to-date contact information for your participants.
2. Set up secure file transfers (SFTP) and forced email encryption (TLS) with your provider and other third parties with whom you exchange sensitive data and emails. (Please ask your Relationship Manager for more information.)
3. Provide security awareness training especially for topics such as phishing.
4. Promptly inform us of any breaches or fraud so we can put additional protections on your account.
5. Use e-delivery for all participant communications and go paper free for statements.

7 steps to better security for participants

1. Register your account with Empower.com.
2. Provide all available email addresses and phone numbers for security alerts.
3. Use a password manager (e.g., LastPass, 1Password, KeePass).
4. Use multi-factor authentication (MFA).
5. Leave MFA enabled by not clicking "remember this device."
6. Pay attention to security alerts.
7. Freeze your credit with the 3 major credit bureaus and only unfreeze your credit for the time you want additional credit.

What to do if you are a victim of fraud

1. Change your password(s), then notify all your financial institutions, including Empower. We can put additional protections on your account.
2. Notify all three major credit bureaus:

   Equifax: **888-202-4025** or equifax.com
   Experian: **888-397-3742** or experian.com
   TransUnion: **800-680-7289** or transunion.com

3. If you are a victim of online crime, file a report with the FBI's Internet Crime Complaint Center (IC3.gov) as soon as possible.

FOR FINANCIAL PROFESSIONAL USE ONLY.

Industry links and resources

SPARK Institute (Society of Professional Asset-Managers and Recordkeepers)
Leading nonprofit association regarded as a major voice influencing federal retirement policy and thought leader for data security.

- Data Security Oversight Board: 16 control objectives
- Cybersecurity conferences and training

NIST (National Institute of Standards and Technology)
NIST develops cybersecurity standards, guidelines, best practices, and other resources to meet the needs of U.S. and global industries, including financial services. NIST CSF provides a cost-effective, adaptable, and flexible framework that any organization can use for creating and maintaining an information security program. NIST 800-53 and NIST 800-171 provide security controls for implementing NIST CSF.

- Quick Start Guide
- Informational Videos
- Awareness, education, training, and workforce development
- Cybersecurity supply chain projects
- Ransomware resources

CISA.gov (Cybersecurity & Infrastructure Security Agency)
All services are available at no cost to federal agencies, state and local governments, critical infrastructure, and private organizations.

- Security assessments
- Cybersecurity training

FBI IC3 (Federal Bureau of Investigation Internet Crime Complaint Center IC3)
Small businesses should immediately report any threats and incidents to the FBI's IC3. The IC3 accepts online internet crime complaints from either the actual victim or from a third party to the complainant.

- File a complaint
- Consumer and industry alerts

Empower's cybersecurity resource library

Please ask your Relationship Manager for these materials

- Empower Recordkeeping Technology and Cybersecurity Guide
- Empower's Response to the DOL's Cybersecurity Guidelines
- Empower Overview DOL EBSA Cybersecurity Guidance
- CISO Cybersecurity Videos
- Co-branded Participant Communications Campaigns
- Whitepaper: Defense-in-Depth Protecting your Plan
- SOC 2 Type 2 + AICPA SOC 2 Overview

FOR FINANCIAL PROFESSIONAL USE ONLY.

Securities, when presented, are offered and/or distributed by GWFS Equities, Inc., Member FINRA/SIPC. GWFS is an affiliate of Empower Retirement, LLC; Great-West Funds, Inc.; and registered investment adviser, Advised Assets Group, LLC. This material is for informational purposes only and is not intended to provide investment, legal or tax recommendations or advice.