The Impact of the Russia-Ukraine War on U.S. Employee Benefit Plans

CARLTON C. PILGER
Of Counsel
Fisher Phillips

Email: cpilger@fisherphillips.com
Phone: (404) 240-4141

Agenda

- Preparing for cyberattack
- Promoting Employee Assistance Programs (EAP)
- Examining your leave policies to accommodate employees who need to address urgent family needs due to the Ukraine crisis
- Understanding the limitations of international benefits and business travel accident coverage during a foreign war
- Preparing for new and unique employment issues

Cybersecurity & Cyberattacks

Cybersecurity & Cyberattacks

- Protecting personal information and other account data is not specifically enumerated as a fiduciary duty in ERISA, however, through recent guidance Department of Labor (DOL) has confirmed that plan fiduciaries have a duty to mitigate cybersecurity risks to their employer-sponsored plans.
- In addition, there is a general fiduciary duty under trust law to maintain confidentiality and privacy of third parties' information except as required by law or needed to administer the plan.
- The purchase of supplemental insurance policies covering cyber-related risks may not be necessary. However, doing so may fill gaps in existing processes and liability coverages and address expanded duties and potential liability.

Cybersecurity & Cyberattacks

DOL Cybersecurity Guidance for Employee Benefit Plans

- ERISA Advisory Council provided initial guidance in 2016 on suggested materials and considerations for plan sponsors, plan fiduciaries, and third-party service providers when developing cybersecurity strategies.
- Government Accountability Office urged the DOL to release guidance on cybersecurity matters in an effort to mitigate risks to 401(k) and other retirement plans.
- April 14, 2021 guidance: DOL did not issue statutory or regulatory guidance, but provided guidance focused on steps that should be taken by plan sponsors and fiduciaries, third-party service providers, and individuals.

Cybersecurity & Cyberattacks

- In issuing this guidance, the DOL recognized that plan fiduciaries have a duty to mitigate cybersecurity risks. The DOL's cybersecurity guidance was released in three parts:

1. Tips for Hiring a Service Provider with Strong Cybersecurity Practices, which provides guidance to plan fiduciaries in the hiring of service providers;

2. Cybersecurity Program Best Practices, which provides best practices for recordkeepers and other service providers; and

3. Online Security Tips, which provides advice to plan participants and beneficiaries who check and manage their accounts online.

Cybersecurity & Cyberattacks

- In brief, the 12-point best practice system identified by the DOL is:

1. Have a formal, well-documented cybersecurity program. This includes a system to identify risks, protect assets, data and systems, detecting and responding to cybersecurity events, recovering from the event, disclosing events, and restoring normal operations and services. This program should be approved by senior leadership, reviewed internally at least annually, and should be reviewed by an independent third-party auditor to assess compliance and threats.

2. Create a prudent, annual risk assessment program. A manageable, effective risk assessment schedule should be established to assess cybersecurity risks and to describe how the program will mitigate identified risks. This program should be updated for changes.

Cybersecurity & Cyberattacks

3. Engage a third-party annual audit of the security controls. An independent third-party auditor should assess the security controls on an annual basis and any corrections must be documented.

4. Clearly define and assign information security roles and responsibilities. Related to the first and second point, a prudent system to manage cybersecurity risks should clearly identify who has responsibility for each aspect of the program.

5. Ensure strong access control procedures. A strong procedure should be established to guarantee that users are who they say they are and that only approved users are able to access IT systems and data. This would require an appropriate system of authentication and authorization.

Cybersecurity & Cyberattacks

6. Assess third-party service provider use of cloud computing. This would include requiring a risk assessment of the third-party service provider, periodically assessing the service provider, and ensuring that the guidelines of any safety program are satisfied.

7. Conduct annual cybersecurity awareness training. Conduct an annual cybersecurity awareness to at each level (including employees) to educate everyone to recognize attacks, help prevent incidents, and guard against identify theft.

8. Implement a secure system development life cycle (SDLC) program. A secure SDLC program ensures that security assurance activities, such as code review, are an integral part of the system development process.

Cybersecurity & Cyberattacks

9. Implement a business resiliency program to address business continuity, disaster recovery, and incident response. Create a business continuity plan, disaster recovery plan, and an incident response plan.

10. Encrypt sensitive data. Implement current, prudent standards for encryption data that is stored and for data that is transmitted.

11. Implement strong technical controls to implement best security practices. Keep hardware, software, and firmware up to date, conduct routine data backup, and ensure routine patch management.

12. Be responsive to cybersecurity incidents or breaches. Ensure appropriate action is taken to protect the plan in the event of a cybersecurity incident or breach.

Cybersecurity & Cyberattacks

- This guidance now sweeps cybersecurity considerations into the topics of consideration when selecting service providers.
- The DOL provides suggested questions to ask potential service providers in order to gauge that service provider's cybersecurity practices. This includes asking the service provider about:
  - their information security standards,
  - audit policies and results,
  - how it validates its practices,
  - what levels of security standards it has met and implemented, and past security breaches.

  The responses should be considered against other potential service providers, industry standards, and the service providers track record.

Cybersecurity & Cyberattacks

- Guidance on the actual review and negotiation process for hiring service providers and considerations in monitoring and assessing the relationship. Contracts should:
  - Require the service provider to obtain third-party audits on an annual basis;
  - Specify the service provider's obligation to keep private information private, prevent disclosure, and meet a strong standard of care to do so;
  - Identify how quickly a service provider must inform plan fiduciaries of breaches;
  - Specify the service provider's obligation to meet applicable federal, state, and local laws regarding privacy, confidentiality, or security of participant's personal information;
  - Include a broad definition of "data security breach" so that it includes "suspected breaches; and
  - Generally, clarify the roles of responsibilities of the vendor and the plan fiduciaries.

Cybersecurity & Cyberattacks

- The final component of the DOL guidance focuses on steps and actions that plan participants and beneficiaries can take to mitigate potential cybersecurity risks on their end.

- These tips include regular monitoring of their accounts, the use of strong passwords with multi-factor authentication, updating personal contact information, and signing up for account activity notices.

Cybersecurity & Cyberattacks

- As part of this advice, the DOL also provides individuals with some general best practice considerations when accessing accounts or having an online presence generally, such as:
  - Routinely monitoring their online account;
  - Using strong and unique passwords;
  - Using multi-factor authentication;
  - Keeping personal information current;
  - Being careful with public wi-fi;
  - Being award of phishing and spoofing attacks; and
  - Using up to date antivirus software and applications.

Cybersecurity & Cyberattacks

- Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) requires mandatory reporting by “critical infrastructure” of substantial cyber incidents and ransomware payments.
- Mandatory reporting requirements for entities in chemical, commercial facilities, communications, critical manufacturing, emergency services, energy, food and agriculture, healthcare and public health, and information technology areas.
- Effective when final rules published, which could take as long as 36 months.

Cybersecurity & Cyberattacks

- These entities must report to the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA):
  - a covered cyber incident no later than 72 hours after covered entity reasonably believes incident occurred, and
  - any payment for ransomware attack within 24 hours of payment.
- Reportable incidents include:
  - a substantial loss of confidentiality, integrity, or availability of a system or network;
  - serious impact on operational systems and processes; or
  - disruption of business or industrial operations.

Cybersecurity & Cyberattacks

- A report of a covered cyber incident under the Act must include:
  - description of affected information systems, networks, or devices;
  - description of unauthorized access;
  - estimated date range of incident;
  - impact to covered entity's operations;
  - description of vulnerabilities exploited and security defenses in place;
  - information related to each actor reasonably believed to be responsible for cyber incident;
  - category of information that was, or reasonably believed to have been, accessed or acquired; and
  - name and contact information of covered entity.

Cybersecurity & Cyberattacks

- A report of a covered ransomware incident under the Act must include:
  - type of virtual currency or other commodity requested;
  - ransom payment instructions, including information regarding where to send the payment, if applicable; and
  - amount of ransom payment.

Cybersecurity & Cyberattacks

- Ten keys to cybersecurity strategy
  - Maintain remote access vigilance, especially with many employees working remotely;
  - Require multifactor authentication to access internal network;
  - Keep security software up to date and install timely systems patches;
  - Enable robust spam filters;
  - Enforce strong, unique passwords with multiple characters (e.g., numbers, letters, and symbols) and require that they be changed routinely.

Cybersecurity & Cyberattacks

- Ten keys to cybersecurity strategy
  - Encrypt data at rest and in transit when possible;
  - Implement robust cybersecurity user awareness and training programs for new workers upon hire and at least annually for existing employees;
  - Immediately disable credentials upon employee departure;
  - Create regular data backups; and
  - Ensure you have strong cybersecurity team in place to not only monitor your network for vulnerabilities and any suspicious activity but also to develop and deploy an incident response plan (which should include response and notification procedures) in the event of a compromised system.

Cybersecurity & Cyberattacks

- Effect of HIPAA Rules
  - HIPAA defines breach as acquisition, access use or disclosure of PHI in a manner not permitted under HIPAA Privacy Rule that compromises the security or privacy of PHI
  - Presumed breach due to security incident, but can overcome presumption by showing low probability of compromise based on following factors:
    - the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
    - the unauthorized person who used the PHI or to whom the disclosure was made;
    - whether the PHI was actually acquired or viewed; and
    - the extent to which the risk to the PHI has been mitigated.

Cybersecurity & Cyberattacks

- Effect of HIPAA Rules
  - Breach reportable if it involves unsecured PHI.
    - Unsecured if not rendered unusable, unreadable, or indecipherable to unauthorized persons through technology or methodology specified by HHS.
    - Encryption satisfies this standard.
  - Breach exceptions
    - unintentional acquisition, access, or use of PHI by a workforce member acting under the authority of a covered entity or business associate;
    - inadvertent disclosure of PHI from one person authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate; and
    - unauthorized disclosures in which an unauthorized person to whom PHI is disclosed would not reasonably have been able to retain the information

Special Leaves of Absence

Leaves of Absence

- Expect to receive employee leave requests to care for affected family members overseas or to engage in humanitarian efforts.
- Ukraine's President's recent rally for foreign volunteers to join Ukraine's Territorial Defense force may trigger employees' requesting leave to join the fight.
- Subject to applicable federal and local laws, now is a good time to re-evaluate your Paid Time Off (PTO), Paid Sick Leave, and/or any other applicable leave policy in order to process such requests.
- It is also prudent to re-familiarize yourself with protected military leave laws in anticipation of further U.S. involvement in the conflict.

Leaves of Absence

- Consider how benefits will be covered for leave ranted in certain situations.
- Communications need to be clear.
- Cases should be handled consistently.

USERRA – The Basics

- USERRA protects employees and applicants in the uniformed services who are called to service
  - "Uniformed services" includes the Army, Navy, Marine Corps, Air Force, Coast Guard, and Public Health Service commissioned corps, as well as the reserve components of each of these services (includes trainings)
  - "Service" includes voluntary/involuntary, active duty, training, fitness for duty exams, funeral honors
- Employers are required to provide up to 5 years of unpaid leave (cumulative)
  - Extensions are available under certain circumstances (e.g. initial enlistments lasting more than 5 years)
  - Employee may use accrued paid leave, but employer cannot require
- Employees returning to work are to be:
  - Promptly reemployed
  - Reinstated with all rights and benefits that they would have earned without the break in employment
  - Protected from discrimination
- Can't discharge employee after return unless "for cause" if leave is > 30 days
  - On leave for 30 days or less → No special protection
  - On leave > 30 but < 181 days → protection for 6 months
  - On leave > 180 days → protection for 1 year

USERRA – Health Coverage

- Uniformed Service Employment and Reemployment Rights Act (USERRA)
  - Employees on leave can continue to participate in employer's health plan.
  - Up to 24 months or the period of service, whichever is less.
  - Employee is responsible for his/her normal premiums during the first 30 days; 102% of premium after first 30 days.
  - Applies to dependent coverage if the employee had such coverage before the leave.
  - Watch for interplay with COBRA (if employer has 20 or more employees); Essentially provide greatest benefit to employee.

USERRA – Health Coverage

- Uniformed Service Employment and Reemployment Rights Act (USERRA)
  - Flexibility for election process and timing; employer should adopt reasonable procedures.
  - Sponsors will want to confirm insurer and stop-loss provider procedures for premium payments while on leave to avoid conflicts.

USERRA – Health Coverage

- Uniformed Service Employment and Reemployment Rights Act (USERRA)
  - *Employee Provides No Advance Notice of Service.* When employee departs for uniformed service without providing advance notice of service, employer may immediately cancel employee's health coverage, but coverage must be retroactively reinstated (without administrative costs to employee) if employee was excused from the advance notice requirement because of military necessity, impossibility, or unreasonableness and later elects and pays for USERRA continuation coverage.

USERRA – Health Coverage

- Uniformed Service Employment and Reemployment Rights Act (USERRA)
  - *Employee Provides Advance Notice of Service; Employer Has Adopted Reasonable Rules Regarding Election Period.* When employee departs for uniformed service (for a period > 30 days) and provides advance notice of service, employer may immediately cancel employee's health coverage, but coverage must be retroactively reinstated (without administrative costs to employee) if employee timely elects and pays for USERRA coverage within period designated in employer's procedures regarding elections (if procedures are reasonable).

USERRA – Health Coverage

- Uniformed Service Employment and Reemployment Rights Act (USERRA)
  - *Employee Provides Advance Notice of Service; Employer Has Not Adopted Reasonable Rules Regarding Election Period.* When employee departs for uniformed service (for a period > 30 days) and provides advance notice of service, employer may immediately cancel employee's health coverage, but coverage must be retroactively reinstated (without administrative costs to employee) if employee elects and pays for USERRA coverage at any time during the employee's maximum USERRA coverage period (up to 24 months).

USERRA – Health Coverage

- Uniformed Service Employment and Reemployment Rights Act (USERRA)
  - Employees entitled to reenrollment upon reinstatement.
    - Immediate reenrollment without any lapse in coverage.
    - No exclusions or waiting periods except for exclusion of service-connected injuries.
- If on TRICARE, no HSA contribution permitted.

Employee Assistance Programs (EAP)

Employee Assistance Program (EAP)

- May see increase in reports of mental health impact as conflict continues.
- Employers with existing Employee Assistance Program (EAP) should send a reminder of counseling and other related benefits.
- Those with no EAP might consider gathering third-party resources and developing a plan to address mental health issues.
- Can help maintain morale and a healthy workplace.

International Health Coverage and Business Travel Accident Coverage

Group Health Plan International Travel Exclusions

- Most group health policies exclude coverage for services rendered internationally while a participant is travelling abroad.
- Employees leaving to travel abroad during this conflict should be advised of the restrictions under their group health plans.
  - Does plan cover emergency expenses abroad such as return to U.S. for treatment if seriously ill?
  - Are pre-authorizations or second opinions required before emergency treatment can begin?
  - Does policy/plan guarantee medical payments abroad?

Group Health Plan International Travel Exclusions

- Exclusions can be tricky as major carriers often differentiate what's covered internationally under specific definitions of "emergency" or "urgent" care.
- Many carriers offer travel insurance to supplement regular health plan coverage.

Business Travel Accident Insurance

- Provides insurance against accident while traveling on company business.
- Principal purpose typically to provide life insurance benefits to employee's survivors if employee's accidental death occurs during business travel, policies also provide payment of part or all of the face amount of insurance to employee if serious injury, such as loss of limbs, occurs during the employee's business travel.

Business Travel Accident Insurance

- Beware of exclusions based on non-authorized travel activities while on business at the time of occurrence of injury or death.
- Check for provisions excluding payment for losses sustained in war or acts of war.
- Carriers can add war coverage rider.

Unique Employer Issues

Reimbursement of Work Expenses

- Employee requests to work remotely at international location – either on a long-term or permanent basis.
- Consider whether employee can competently and efficiently perform their work remotely.
- Assess legal obligation to reimburse employees for costs incurred as a result of working remotely.
  - Important to know where employees are located to determine applicable laws, decide whether to permit employees to work from those locations and develop policies and practices that comply with applicable laws.

Reimbursement of Work Expenses

- Generally, laws of country where employee performs services will apply to employment relationship.
- The longer employee works from another country, the more likely local law will apply.
- Knowing employees' location is important because laws vary widely.
  - United Kingdom, Canada, India, and Australia impose no legal obligation on employers to reimburse employees for expenses employees incur while working remotely.

Reimbursement of Work Expenses

- Knowing employees' location is important because laws vary widely.
  - Spain, Brazil, Italy, and China impose general requirement that employers must reimburse employees for any business expenses including equipment employees need to work remotely, such as computers and desks.
  - Colombia, the Czech Republic, France, and Mexico require employers to reimburse employees for all remote work expenses including a proportionate share of the employees' utilities costs.

Reimbursement of Work Expenses

- Knowing employees' location is important because laws vary widely.
  - Japan, South Africa, and New Zealand have no explicit statute requiring employers to reimburse employees for remote work expenses, but reimbursements are highly recommended to avoid claims of discrimination or claims based on negative changes in working conditions.
- Determine whether a locale has applicable federal, regional, municipal, or other laws that apply, and if so, how they intersect.
- Opt for one global policy including most comprehensive and generous requirements for all employees regardless of geographic location, or basic global policy with individually tailored policies that cover employees who work in areas with more stringent rules.

Reimbursement of Work Expenses

- Carefully consider employees with individual employment contracts so policies do not materially change contract terms and be deemed to breach contract or lead to constructive discharge – potentially costly unintended consequences.

Thank You

CARLTON C. PILGER
Of Counsel
Fisher Phillips

Email: cpilger@fisherphillips.com
Phone: (404) 240-4141

Final Questions

Email: ubamember@fisherphillips.com

HRCI –

SHRM –

CARLTON C. PILGER
Of Counsel
Fisher Phillips

Email: cpilger@fisherphillips.com
Phone: (404) 240-4141