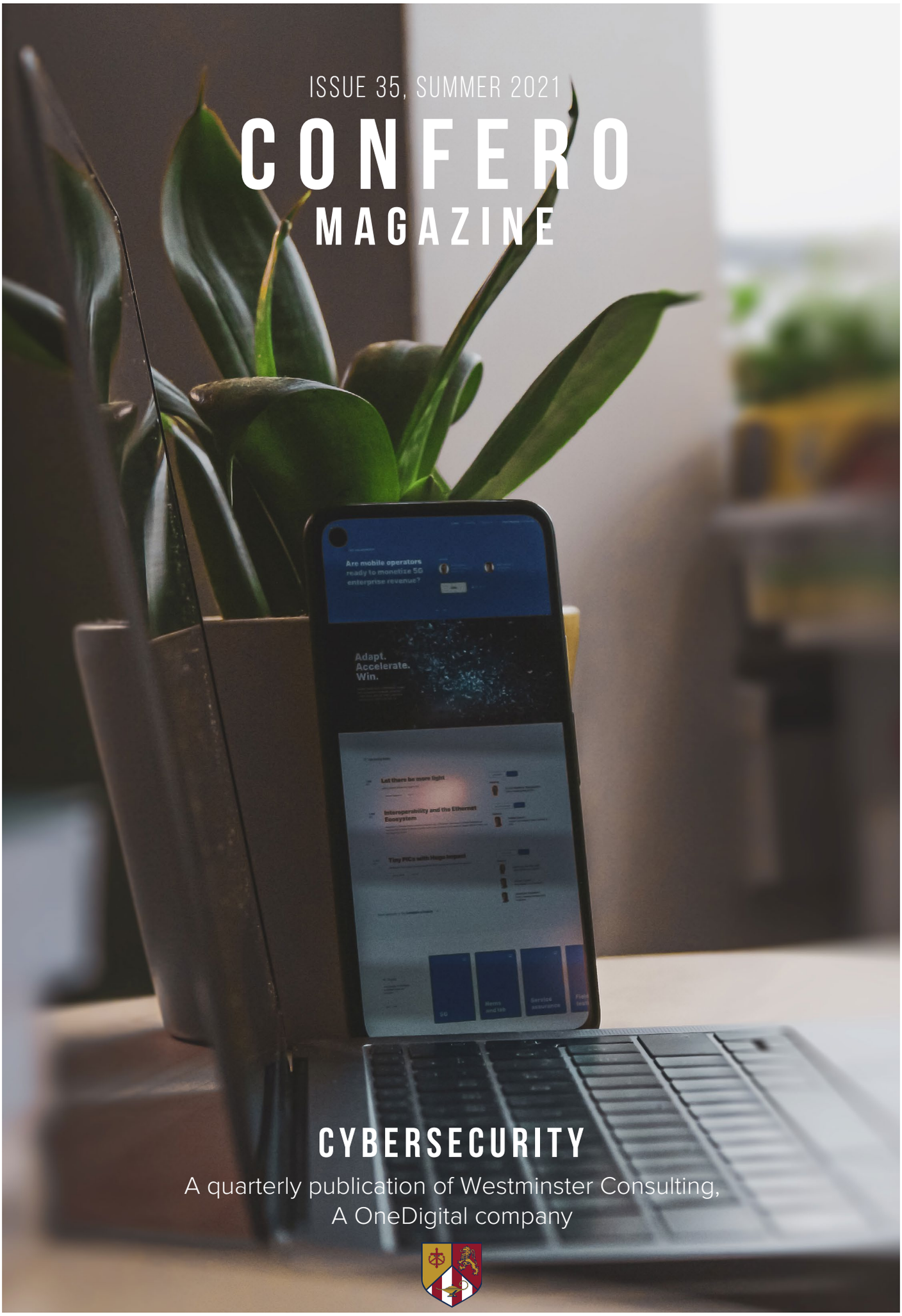
ISSUE 35, SUMMER 2021

CONFERO
MAGAZINE



CYBERSECURITY

A quarterly publication of Westminster Consulting,
A OneDigital company

MITIGATING CYBERSECURITY RISKS FOR RETIREMENT PLANS

BY MICHELLE CAPEZZA, ESQ.

On April 14, 2021, the U.S. Department of Labor's Employee Benefits Security Administration (EBSA) issued its first formal cybersecurity best practices guidance for retirement plans, which had long been anticipated by the benefit plan community. The EBSA guidance is set forth in three parts, including (i) Tips for Hiring a Service Provider with Strong Cybersecurity Practices, (ii) Cybersecurity Program Best Practices, and (iii) Online Security Tips. In the Cybersecurity Program Best Practices guidance, EBSA states that "[r]esponsible plan fiduciaries have an obligation to ensure proper mitigation of cybersecurity risks." It is the first formal pronouncement from EBSA that ERISA plan fiduciaries are at least obligated to ensure proper mitigation of cybersecurity risk.

"[R]ESPONSIBLE PLAN FIDUCIARIES HAVE AN OBLIGATION TO ENSURE PROPER MITIGATION OF CYBERSECURITY RISKS."

This three-part guidance can assist plan sponsors and fiduciaries with their responsibilities to prudently select and monitor service providers by providing considerations they can use to determine that service providers follow strong cybersecurity practices, issues to address in service agreements, and points to educate participants about so that they can reduce the risk of cybersecurity attacks and threats to their retirement accounts. EBSA views this guidance as a complement to its regulations on electronic records and disclosures to plan participants and beneficiaries (e.g., that electronic recordkeeping systems have reasonable controls, that adequate records management practices are in place, and that electronic disclosure systems follow measures that protect personally identifiable information). The new guidance is a step forward, as it provides best practices and approaches to mitigate cybersecurity risks and further validates steps that have already been adopted by many plan sponsors and fiduciaries, as well as service providers.

TIPS FOR HIRING A SERVICE PROVIDER WITH STRONG CYBERSECURITY PRACTICES

These tips can assist plan fiduciaries in developing prudent decision-making processes in selecting plan service providers and monitoring them on an ongoing basis. Plan fiduciaries should review the service providers' cybersecurity practices when selecting them, including publicly available information regarding incidents, and levels of insurance. Ongoing monitoring practices should also be developed to determine compliance with cybersecurity and information security standards. The guidance provides examples of questions to pose to service providers, and information to review, when vetting them such as those concerning their security practices, breach incidences, audit results and reports, litigations, and insurance coverage. In addition, the guidance provides that service agreements should establish contractual terms for data breach notifications; compliance with all applicable federal, state, and local laws, rules, regulations, directives, and other governmental requirements pertaining to the privacy, confidentiality, or security of participants' personal information; and insurance coverage.

It would also be prudent for plan fiduciaries to review the terms of any guarantees offered by service providers to cover losses of account assets due to cyber theft which occur through no fault of the participant, communicate those terms to participants, and to the extent possible, their availability should be cross-referenced in the service agreement. Any liability caps, and the scope of contractual indemnification terms, should also be reviewed and negotiated as they relate to protections for breaches of cybersecurity, including those which result from third-party actions, such as agents and subcontractors, along with any additional desired protections. It would be prudent for plan fiduciaries to obtain their organization's general data privacy terms or addendum used for vendor contracts and request that it be added to the plan service agreement. Alternatively, request such an addendum from the service provider so that it can be reviewed and negotiated as needed.

CYBERSECURITY PROGRAM BEST PRACTICES

While primarily addressed to service providers handling plan-related IT systems and data, this guidance imposes upon plan fiduciaries the obligation to ensure mitigation of cybersecurity risks by conducting proper due diligence when selecting service providers to confirm their adherence to prudent cybersecurity practices and procedures to indicate that plan participants' information, data, and accounts will be safeguarded on an ongoing basis, that appropriate controls are in place, and that responsible cybersecurity breach response procedures are followed. Plan sponsors and fiduciaries should determine who will assist them in evaluating their service providers' cybersecurity practices such as by reviewing their policies, audit reports of security controls, and responses to cybersecurity inquiries.

Among other best practices, this guidance provides that plan service providers should have formal, well-documented cybersecurity programs; conduct prudent annual risk assessments; obtain reliable annual third- party audits of security controls; conduct periodic cybersecurity awareness training; have access controls and use data encryption; require third-parties to have and define their adherence to security standards; have up-to-date firewalls, hardware, software, routine patch management and hardened systems against attacks; implement and manage a secure system development life cycle (SDLC) program; have appropriate business continuity, disaster recovery and incident response procedures; and maintain responsive cybersecurity breach and incident response plans and procedures. As part of an SDLC program, it is important for the service provider to be able to demonstrate that there are measures to trigger additional validation and authentication procedures when participants change personal information, especially if they do so prior to a distribution request. Plan sponsors and fiduciaries should discuss with their service providers, and document, the agreed-upon data breach notification and related procedures that can be implemented in the event of a data breach.

ONLINE SECURITY TIPS

This guidance provides tips regarding how participants can help reduce the risk of cybersecurity attacks and threats to their retirement accounts. Among these tips, EBSA advises plan participants to use strong passwords and multifactor authentication, as well as how to be aware of possible phishing attacks that may expose their retirement accounts to cybersecurity breaches.

Although directed at plan participants, plan fiduciaries should be cognizant of what tools, procedures, and possible educational trainings they can offer to their plan participants to aid in mitigating cybersecurity risks. Ongoing communication and education on these issues will help mitigate risks.

NEXT STEPS

The EBSA guidance is a step forward in expressing its view on the respective responsibilities among plan sponsors and fiduciaries, service providers, and plan participants when it comes to cybersecurity and retirement plans. The concept that plan sponsors and fiduciaries have a responsibility to ensure mitigation of cybersecurity risk should serve as a call to action to revisit existing service provider relationships and update agreements, request the necessary information to evaluate the state of their benefit plan cybersecurity practices and procedures, document cybersecurity policies that will be followed to safeguard participant information, data and accounts as well as data breach response procedures, and incorporate this type of review on a go-forward basis with new and existing service providers. The DOL has already commenced its audit initiative on cybersecurity and plan sponsors and fiduciaries must be prepared to respond.

These issues should also be addressed for all benefit plan programs where participant information and data is handled, processed, transmitted and stored, in accordance with all applicable laws. New laws, regulations and litigation will evolve in this area, and the scope of plan fiduciary responsibility will be further shaped. Plan sponsors and fiduciaries should continue to monitor these developments and update their processes and procedures accordingly.