Control of Work Product in the Digital Age

It's good practice for pension professionals to take steps to control their work products and minimize the risks that come with modern technology.

BY LAUREN BLOOM

The highly publicized Internet theft of confidential information from Sony Pictures last year was an object lesson in the risks of doing business in a digital world. According to news reports, foreign hackers who were offended by one of Sony's films broke into the company's computers and stole as much as 100 terabytes of data, then installed malware into the servers, wiping essential data from Sony's systems. The entertainment giant suffered massive trouble and embarrassment as upcoming films were released early online, reams of confidential information about its employees (including names, addresses, salaries, and Social Security numbers) were posted, and catty internal emails became fodder for public gossip.

Most pension professionals won't be targeted by hostile foreign hackers. However, the Sony incident highlights the importance of thinking carefully about control of work product that is created, delivered and maintained in electronic form. These days, it's all too easy for confidential participant data to be stolen, or for a professional's work product to be edited without permission, misquoted, used for a purpose the pension professional never intended, or circulated to third parties without the pension professional's approval. It's good practice for pension professionals to take appropriate steps to control their work products and minimize the risks that come with modern technology. Section 7 of ASPPA's Code of Professional Conduct provides specific, relevant guidance:

> *A Member shall not perform Professional Services when the Member has reason to believe that they may be altered in a material way or may be used to violate or evade the Law. The Member should recognize the risk that materials prepared by the Member could be misquoted, misinterpreted or otherwise misused by another party to influence the actions of a third party and should take reasonable steps to ensure that the material is presented fairly and that the sources of the material are identified.*

Luckily, there are many steps that pension professionals can take to control their work products in the digital age. Following are just a few.

Install security systems and protocols. The nature of their work guarantees that pension professionals have routine access to mountains of confidential information about plan participants and, often, plan sponsors. It just makes good sense to have IT security systems in place to thwart hackers who may try to steal data from computer systems, and to store data securely after use. It's smart to make sure that confidential client data is transmitted securely. It's also a good idea to design internal systems and procedures so that access to client data is granted only to employees who need it to do their jobs.

Educate your clients. Despite regular news reports about cybersecurity breaches, many people continue to hit "send" without thinking carefully about what they're sending and who might be affected by it. It's wise to teach clients not to use your work products for other than their intended purposes, not to send them to third parties without your express, written permission, and never to quote your work in part if it can only be understood in full. Consider putting appropriate controls on the use of your work in your engagement letters, and remind clients periodically about them.

Encourage questions. If you think there's a risk that your client, or some authorized user, may misinterpret your work product, make an extra effort to encourage them to contact you for clarification.

Caveat your work product. Even if you give clients clear guidance on how to use your work, it's all too easy for e-documents to find their way into the wrong hands. Depending on the nature of the work product, it may be smart to include descriptions of who can use the work product and to what purpose, specific statements that the work is not to be altered, excerpted or misquoted, and directions on where to go for additional information or answers to questions. It's also important to satisfy Section 7's requirement to take reasonable steps to ensure that material in the work product is presented fairly and that the sources of the material are appropriately identified.

PDF your work products – and keep a copy. These days, there's no such thing as the electronic document that can't be digitally altered. Still, it's normally prudent to send work products in a format that makes tampering more difficult, and to keep copies of the originals for a reasonable time after you send them. Thankfully, secure digital storage is readily available, making stacks of dusty files a thing of the past. Consider putting a document retention policy in place if your firm doesn't already have one, and keep e-documents just as you would paper.

Train your staff. Inexperienced employees may be so accustomed to sharing information online in their personal lives that they don't consider how work products can be abused online. Put policies in place to prevent inappropriate transmission of data and work products, train your employees on them, and check periodically to make sure they've gotten the message.

Sony Pictures is a huge multinational corporation with, presumably, state-of-the-art cybersecurity systems. That hackers were able to break into Sony and generate such havoc proves that no one is completely safe online. However, with thought and care, pension professionals can reduce the risk that their work products will be misused, boosting client confidence and demonstrating their own professionalism. PC

Lauren Bloom is the General Counsel & Director of Professionalism, Elegant Solutions Consulting, LLC, in Springfield, VA. She is an attorney who speaks, writes and consults on business ethics and litigation risk management.

» Public Pension Plan Insights

(continued from page 27)

topic that many public pension plans hold dearly, but in my opinion, does more harm than good: the "contract clause."

Under the contract clause, in many states, the plan participants retain the right to all plan provisions in place at date of hire — for all past and future service. Because of the contract clause, changes to plan provisions that lower funding — and even ones that would eliminate provisions that are being abused — can only be made prospectively, for new employees. This roadblock provides some strong ammunition for the contrarians that state DB plans are too rich.

CONCLUSION

There is no broad-brush stroke that can paint a picture of all public pension plans. Many public pension plans operate in a manner that controls risk while providing a safe, secure and affordable benefit to millions of participants. The plans that are in trouble are the ones that have promised unreasonable benefits, allowed participants to game the system with outdated — and possibly even careless — provisions, failed to provide adequate investment oversight and did not make adequate contributions.

So the next time someone makes a statement that all public pension plans are in trouble, think about the potential issues and how, like most issues in our society, the answer is never as easy as it seems. PC

The views expressed in this article are those of the author(s) and are not necessarily the views of FTI Consulting, Inc., its affiliates, subsidiaries, management or its other professionals.

Joseph A. Nichols, MSPA, ASA, EA, MAAA, is the Senior Director, Pension Consulting Services, at FTI Consulting in Savannah, Mo. Joe has provided pension actuarial services to a wide range of plan sponsors for more than 25 years. He is the president-elect of ASPPA.