

I am John W. Barton, CEO of a third party benefit and health program administrator in Dublin, CA.

We administer 17 plans, including health and welfare, retirement, and voluntary programs—primarily for Taft-Hartley plan sponsors but also for single employers and unions. I am not a cybersecurity expert; I am a generalist, trained at Stanford Business School (MBA), with a background in human resource consulting at Mercer Human Resource Consulting.

We have been in business since 1989, when we were incorporated as a for-profit company. Prior to that year our staff was employed by a trust fund as their in-house administrator. The change came about so that the company could win additional clients, grow the revenue stream, and support newer technology and new management talent as the demands of the business became more complex.

I believe you asked me here to discuss the implications of new/additional rules for cyber security and privacy in general. Presumably the objective is to assure plan participants that the information obtained and maintained by ERISA-sponsored plans will be secure at all times and in all scenarios—or as nearly so as possible.

I have a few judgements to share with you, which I hope will be helpful to your deliberations.

Participants are mindful of the need to protect their information. They are concerned about identity theft, for obvious reasons, and they are equally concerned about the implications of HIPAA for fear that their employers will learn about their health status. The focus on wellness, disease management, and absenteeism in the workplace is making employees with any health condition concerned about the risk of discrimination or other unfair treatment based on their health status. The feedback we get from plan participants in focus groups on this issue is vivid and pointed; they know what HIPAA is.

For plan administrators and other parties concerned about the privacy of data the HIPAA requirements (2003) and HITECH requirements (2009) amount to an intense regime of controls and standards which, if abided by, assure plan participants that their Protected Health Information (PHI) is secure. To assure the security of the data we abide by the following rules:

- we have Business Associate Agreements with all providers of service assuring that information shared between us will be safeguarded as required by federal regulation.

- We all agree in these contracts that there will be no unauthorized use or disclosure of PHI under any circumstances. Even internally such information is shared only on a need-to-know basis.

- We use the PHI only to the extent necessary to satisfy the Business Associate's obligations.

- When possible we aggregate data for operations/evaluation purposes.
- Any electronic transaction or transmission of data must be encrypted.
- Only the minimum data necessary to fulfill any one function is available to that function.
- We have a designated Security Officer whose job it is to provide extensive training on the procedures and to interpret the rules as questions arise.
- We have disaster recovery standards that provide for reviving our business procedures in short order and which provide for the protection of data when damage to the storage facility occurs.
- All security incidents are reported and reviewed.
- When data is no longer needed we destroy it.
- Our risk management procedures are reviewed regularly.

We have applied the HIPAA security standards to all of our business. It is easier to maintain one standard procedure than it is to have two or more regimes which might create confusion and misunderstanding and risk.

Our network security involves three layers. One vendor runs a Managed Intrusion Prevention Service, which notifies us 24 hours a day, seven days a week, of possible intrusions and actions taken to prevent the intrusions. Web access is restricted to approved web servers.

We also have an e-mail firewall which prevents 98% of all e-mail from entering our network. Most of it would be spam, but in some instances we reject large documents from unknown sources and then have to engage in special procedures to admit them once they have been vetted and approved—a cumbersome process of remediation that applies even to long-time vendors or providers of service on occasion.

And we have a service that monitors all activity on an exchange server.

In other words, we PREVENT, PROTECT, and REMEDIATE in a continuous process that entails substantial fees, hardware and software investment, and extensive time commitments from our staff.

If you are considering new rules, new standards, I would encourage you to consider the following:

-please approach any new standards such that we won't have separate security regimes for pension and health and welfare plans. The HIPAA security requirements are detailed; so far as I know everyone in the industry, and certainly the business partners with whom we are working, honors the rules and the reasons for them. New rules will create confusion, require separate measures for different plans, and result in additional expenditures.

-please be aware that the issue of cybersecurity is evolving. The cost of such security will not decline, and in fact new costs are emerging. Example: many of our trust fund clients are being asked by their insurance brokers/counsel to consider buying cybersecurity coverage. We have recently purchased it for our company. The coverage includes provision for:

- Privacy Notification Expense
- Crisis Management Expense
- Reward Expense
- E-Business Interruption
- E-Theft Loss
- E-Vandalism Expense

The application we had to fill out to qualify for coverage is instructive. The questions included:

- size of our revenue and types of business
- information about our written privacy policy, including if it had been approved by counsel, whether the policy makes provision for notice to affected individuals that their identity is compromised in some fashion, whether we have recently been audited for compliance, whether we accept credit card payments, whether we use and regularly use anti-virus software, how we monitor security vulnerabilities, whether we store or share medical information electronically, whether we outsource payment processing in part or altogether, our forms of data backup, our controls on access, whether we have ever been investigated by regulatory authorities for potential violations of standards, the number of records we have on hand...THIS TO OBTAIN THE COVERAGE.

The challenges are expanding:

- more and more business will be done online
- much of the online activity entails improved communications with plan participants and education about their benefits and payments—essential to wise consumption decisions
- new convenient devices like smartphones and tablets increase our connectivity
- service providers are increasingly interconnected. As a consequence everyone in the chain is vulnerable to attack on the weakest link in the chain of data custody.

-malicious actors are getting smarter.

But tight control can also restrict efficiency, quality of service, response to need. In other words, the issue is not purely technical; it has broad strategic implications that entail tradeoffs between strict security and communication/education/execution to the needs of participants. We do and will continue to limit access to production systems and data so that developers and infrastructure managers won't have access to the live data. But the strategy discussions around data management are broader than they were when we focused only on security. The questions we need to answer include:

-who is responsible for what?

-what information is critical and what is the cost of breach?

-how do our customers view the issue of value with respect to the data?

-is our approach evolving or should it be?

-are we controlling our vendor and partner relationships?

-what security/protect is the IT industry providing and how do we keep pace with the new forms of security required or available?

LET ME CLOSE WITH RECOMMENDATIONS

-It would be helpful to have a national clearing house on risks and risk abatement. I am not sure how you secure the education from bad players, but perhaps a qualified secure entry system for players who are responsible for ERISA-governed plans would be a way to protect the information/guidance.

-It makes sense to have a reinforced federal cybersecurity regime that provides broad protections and allows us to install standardized safeguards.

-Before you initiate any new security requirements consider whether the HIPAA requirements already in place aren't sufficient or at least the proper framework for initiating new standards.

THANK YOU.