STATEMENT BY TIM OXBOROUGH-POWELL
Before the ERISA Advisory Council on
Cybersecurity Considerations for Benefit Plans
August 24, 2016

CYBER SECURITY. ERISA

PERSPECTIVE

It's a risk, along with others, that must be managed. As with all other risks, fraud, fire, etc, the risk can never be eliminated, only managed.

There can be no 'one size fits all" - different organizations have different risk profiles.

The devil is in the details. Conceptually Cyber Security seems straightforward, but it impacts everyone who uses IT, i.e. the whole organization. Hackers realize this: security is only as strong as its weakest link, and they'll attack the weakest, easiest to exploit link, which are often the end users.

Security is 'a journey, not a destination'. It's an 'arms race', so technologies and tools that were good enough last year, won't be in two years' time. Also, since it's mainly a people problem, people need to be constantly reminded about what they should and shouldn't do: e.g. don't click on unknown links.

Security can't be thought of as a layer on top of everything, but needs to be integrated into employees 'business as usual' activities. Most people will 'do the right thing' if the program:

- Is clearly articulated and understood (they know what they should do);
- Not *too* onerous (or else people *won't* comply);
- Enables people to do the 'right thing' (or else people *can't* comply)

The information security program must address these issues.

The 'tone from the top' is critical. If people see leadership breaking/circumventing the rules, they will too.

ROADMAP TO HELP

The remit and resources of the Council will determine how far we can go.

There are many security frameworks that can be leveraged: NIST is a US Government set of standards, as recognized, it is a good place to place to start.

Suggest 'boiling down' NIST (mainly SP 800-53) to:

- Serve as the basis for contractual agreements between large organizations, e.g. between GM and its 401k and healthcare providers. (Large organizations will have robust IT Security programs in place, so it's a question of mapping requirements.)
- Provide a security baseline for any COTS (Commercial, Off The Shelf) packages and systems
- Develop a set of security materials ('Dos and Don'ts, training, etc.) for small and medium sized organizations that don't have an ISO function.

It would also help define a potential set of 'accelerators' to allow organizations to implement security: tools, set of standard security questions to ask 3rd parties, with supporting contractual language.

STATEMENT BY TIM OXBOROUGH-POWELL
Before the ERISA Advisory Council on
Cybersecurity Considerations for Benefit Plans
August 24, 2016

We know that organizations have to comply with other, privacy/security based regulations, e.g. GLBA, HIPAA, so whatever is proposed needs tie into these.

In addition, we know enough about the particular risks to highlight key requirements, e.g. encryption (which can be tied into NIST/FIPS), strong authentication etc.

The initiative can't be just a 'check the box' exercise. It must fit into a broader IT Government, Risk and Compliance program.