



ERISA Advisory Council

August 24, 2016

Presented by
**Brian Smith, COO and
Matthew Jackson, SVP**

 Segal Select Insurance

Cyber Liability—What Is It?

- Preparing for the likelihood that “sensitive information” or “proprietary information” will be improperly handled or disclosed
 - “Sensitive Information” or “proprietary information” generally consists of either
 - Personally Identifiable Information (PII), or
 - Protected Health Information (PHI)
 - Specific national or state laws broadly define these terms
- Specific national or state laws establish breach event responsibilities and liabilities
- For some ERISA benefit plans, foreign laws, such as Canada, may also be applicable



Why Is It Important?

Cyber threats:

- Are not going away
- May capture major media attention
- Cyber threats will increase and become more sophisticated

Cyber breaches can be disastrous at many levels

- For the individual, whose information has been breached
- For the entity
 - As it investigates, corrects, and complies with applicable laws
 - In fines, penalties, and corrective actions that may result
 - In the form of Reputational Risk



What Can You, a Plan, Do?

Apply the Risk Management Model:

- Identify risks
- Manage and mitigate risks
- Transfer any remaining know and unknown risks

Other Steps

- Establish support and need at the Board of Trustees level
- Establish a Cyber “team” and “plan”
 - For the “team” consider a trustee sub-committee consisting of the Plan Administrator, IT, and legal counsel
 - For the “plan,” consider
 - Best practices
 - » These will continuously evolve
 - Identify who does what and when
 - Employee education and accountability
 - Testing
 - Periodic review and updates

**Anticipate
rather than
React**



How Do I Identify the Risks

- Ask questions
- Research and education
 - Many vendors and websites are now available as resources
- Talk with legal counsel, IT, your insurance broker
- Identify all applicable laws
 - Federal and State
- Perform a risk analysis on a regular basis
 - This is also a HIPAA security rule administrative safeguard requirement



How Do I Mitigate Risks

Understand your data

- What PII and PHI do you have?
 - Is there any other data that might qualify as information needed to be protected? For example, do you have any Canadian data? Other proprietary information (trade secrets)
- Where is it stored?
- Who has access?
 - Goal should be “minimum necessary access.”
 - If vendors, what contractual provisions have been negotiated? Have you assessed vendors security program and controls?
 - Remember—you are responsible for your vendors.
- How is it protected?
- How long to you keep data?

In mitigating risks, IT “solutions” such as software, firewalls, etc. may/do exist

- IT staff and/or vendors are critical in this process

What is the Value of Transferring Risks?

- It is a critical step in the Risk Management Module.
- It can help balance costs
 - Elimination and/or mitigating involves scalable costs
 - At some point, transference may be more economical
- Vendor contracts are both a type of mitigating and transferring risks
- Insurance is the ultimate transfer and safety net
 - It is designed to cover both known and unknown risk issues



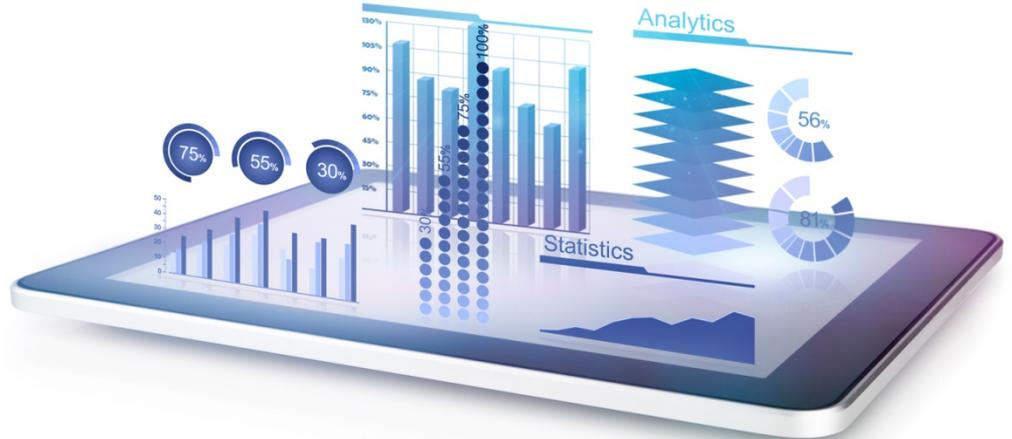
Insurance

- Policy language and scope of coverage vary between and among insurance carriers
 - Policy language evolves over time
 - Currently, carriers are interested in writing this coverage
- Insurance carriers may come in and exit this insurance coverage, cyber liability insurance, based upon its experience with an individual client or the overall “book of business”
- Their “underwriting information” focus varies



Insurance—Points to Consider

- What limit of liability should be purchased?
 - Is it one aggregate limit or do separate limits of liability exist?
- What is the scope of coverage?
- How are claims handled?
- When and how should a claim be notified?
 - Don't wait until you need it
 - Learn how to maximize and leverage the policy before you need it



Recommendations/Items for Consideration

Can the DOL clarify whether ERISA pre-emption applies?

Can the DOL provide either:

- Regulations that will create a single, national breach reporting standard for all employee benefit plans
- Guidance that will provide trustees and administrators better clarity regarding:
 - Whether cyber risk security is a trustee priority or not?
 - If yes:
 - Just how much of a priority is it?
 - Are there certain minimum steps that should be taken?
 - Consider a framework mandate or guidance
 - Finally, as ERISA mandates trustees try to minimize administrative expenses,
 - » Should cyber liability insurance be considered?
 - » Will the cost of cyber liability insurance be a reasonable plan expense?
 - » Given the given the growth, prevalence, and potential disastrous consequences of a significant cyber breach event, could the lack of cyber liability insurance ever be considered a breach of fiduciary duty?

Cyber Liability Insurance—Points to Consider

- Many plans are reluctant to buy it
 - Need for this insurance is not properly understood
- Other insurance policies do not fully respond
- Scope of cyber liability insurance, especially the first party services and coverages, is not properly understood
- Cost of a broad \$1 - \$2-million “safety net” policy is reasonable and competitive



Reasons Given for Not Buying Cyber Liability Insurance

- It is not required
- It is too new
 - We have no evidence it will work and pay claims
- We have never had a claim
- We are not subject to HIPAA/HITECH
- We use a TPA
- We have strong security systems in place
- We have strengthened our vendor contracts
- It is too expensive

