CYBERSECURITY SEMINAR: BREACH SCENARIOS

ABA EMPLOYEE BENEFITS COMMITTEE – 2018 MIDWINTER MEETING

Joseph N. Kravec, Jr., Feinstein Doyle Payne & Kravec
Diane R. McNally, Segal Select Insurance
Karla M. Campbell, Branstetter Stranch & Jennings
Miguel Eaton, Jones Day

February 8, 2018

BREACH SCENARIO #1

- On Monday morning, the FBI notifies you that the Florida company whose plan you recently started administering has suspicious activity on its computer network. According to the FBI, the suspicious activity started approximately 2 years ago, long before you became plan administrator, but the vulnerability was transferred to your network when you received the participant data from the employer.

The impacted computers were used to enter employee benefits data and other personal information. Retiree data was also included on the impacted computers.

BREACH LESSONS LEARNED

- You immediately launch a forensic investigation and determine that personal information including bank account numbers and SSNs of over 100,000 employees and retirees has been accessed. You also learn that employee and retiree benefit and payment data appears to have been exfiltrated.

The employer stored the impacted data in unencrypted databases on its network. The Plan encrypted the data when it received it, although the transferred vulnerability still made it accessible to the hackers.

BREACH PLANNING PRACTICES

- You look at your incident response plan, assemble your team and decide whether to contact your insurance carrier to tell them about the FBI report and your findings so far.
- You look at the applicable data breach notification laws, decide when and how to notify plan participants, including what to tell them and what else you should do as plan fiduciary requires.

Members of the team are concerned about the implications of notifying the insurance carrier and plan participants before fully investigating the incident.

BREACH INCIDENT PLANNING

- Numerous media sources including Krebs on Security begin publishing articles that employee data is for sale on the Dark Web. Local television and newspaper are demanding statements.

The head of communications is on vacation and her right hand manager is on maternity leave. An employee who started last month is trying to handle communications.

WATCH FOR INTERNAL INCIDENTS

- The Plan Administrator sends an email to all employees regarding the incident that states the following: If we rewind the tape, our security systems could have been better. Data security just wasn't high enough in our mission statement. The bottom line is that our data security systems were desperately out of date.

A disgruntled employee sends a copy of the Plan Administrator's email to the local press.

INCREASED BREACH LITIGATION

- A plaintiff's class action firm sees the considerable negative media about the breach and sends the company a draft complaint he intends to file.
- A state AG's office sees the same media and wants to know why the data was not encrypted, and why they were not told sooner. The Department of Labor also inquires.

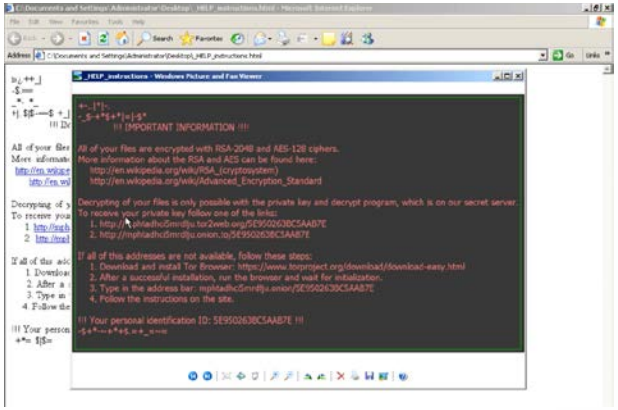
The Plan is on notice of litigation and a possible regulatory investigation.

BREACH SCENARIO #2

- The Plan's health insurer MediSure sustains a data breach of 50 million insureds personal, financial and health data ("PII"). The MediSure data breach contains PII for 32,000 plan participants for a plan your administer.
- MediSure notifies the Plan Administrator of the data breach at the same time as it notifies your plan participants.

PHISHING SCHEME

- Employees and retirees begin calling the Plan Administrator after receiving MediSure's data breach notice.
- The breach was caused when a MediSure employee opened a link on an phishing email that appeared to be from the CEO and installed randonsomware.
- MediSure paid the cyber thieves because its back-ups were company-wide and would take days to re-install.



ISSUES – NOTIFICATION OF THE BREACH

- Initial steps in response to Scenario?
- Notification to plan participants?
- What should the notification letter say?
- Should the Plan offer credit monitoring?
- Should the Plan notify others (*e.g.*, government regulators, the employer, its board of directors, insurance carriers, etc.)?
- Who should conduct the forensic investigation?
- What insurance applies and what does the carrier require?

ISSUES – PLAN PARTICIPANT CLAIMS

- Can Plan participants avoid ERISA; what claims can they bring?
- Can Article III standing to sue in federal court for state law claims exist absent ERISA?
- Can participants sue as a class without ERISA?
- How can the case be settled?

ISSUES – OTHER SUITS

- Risk of lawsuits by financial institutions, e.g., banks or credit card companies
- Risk of shareholder lawsuits
- Risk of action by regulators, state AGs and/or federal agencies
- Risk of lawsuits by employees and retirees
- What claims does the plan have against the employer (if different)?

ISSUES – THIRD PARTY PROVIDERS

- What are the implications of a third party provider breach?
- Was the third party provider's cybersecurity protocols investigated by the Plan before selecting the provider?
- Does ERISA preemption apply to claims from a third party provider breach?
- What steps should the Plan take after being notified of a third party provider breach?

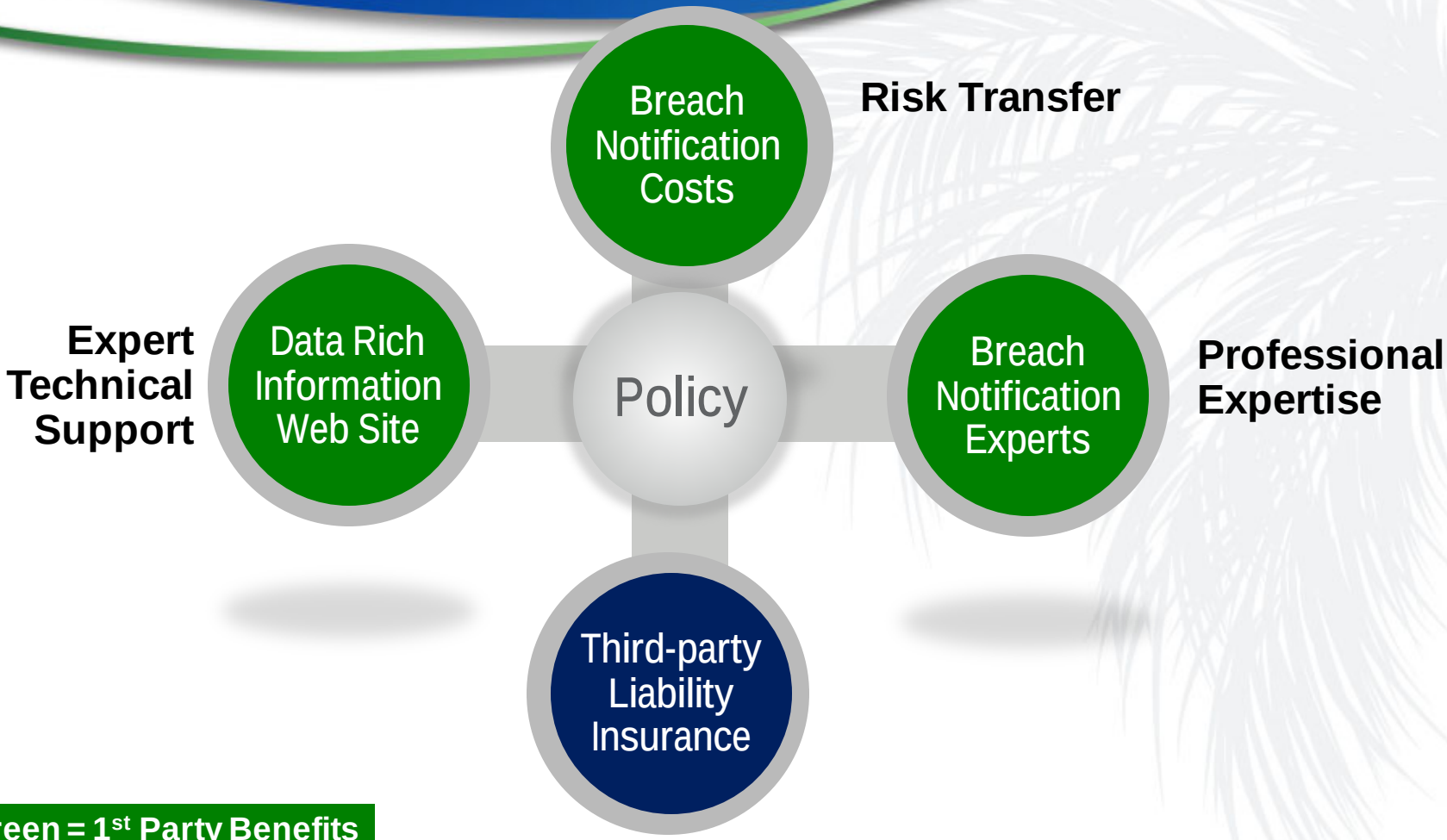
LESSONS LEARNED

- Cyber due diligence in connection with data security and acquisitions is essential
- A battle-tested incident response plan is critical
- Having competent forensic experts lined up in advance of an incident increases effectiveness of response
- Knowing when to notify your cyber liability carrier and affected individuals is critical
- Having a standalone cyber policy is critical
- Proper storage of back ups as well as network segmentation will help in ransomware attacks
- Cyber training for all employees can help to increase awareness, especially of phishing attacks

THE ROLE OF CYBER INSURANCE

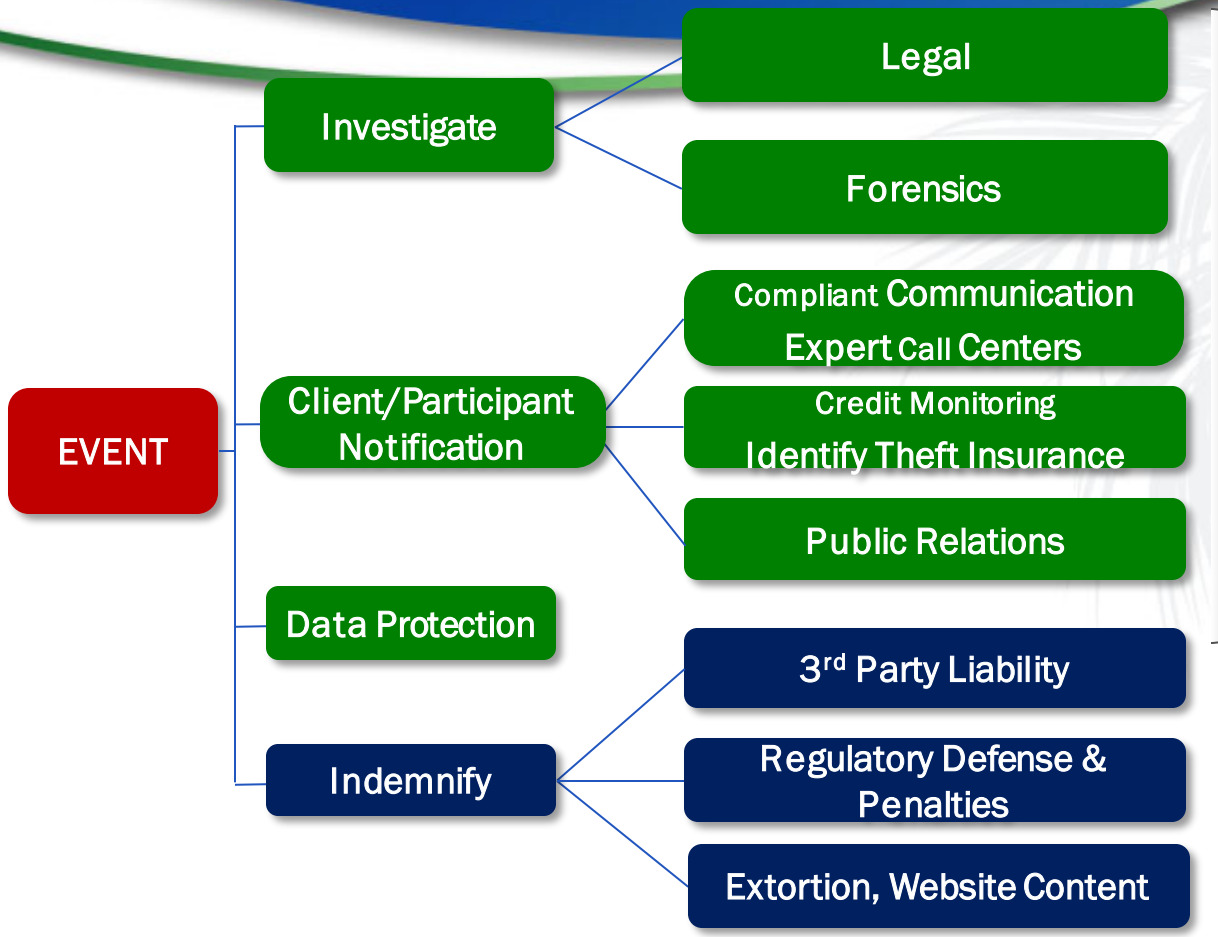
- Designing a policy that protects against cyber exposures
- Adequate 1st party coverage not available elsewhere
- 3rd party coverage relating to data incidents
- Not just expense and liability coverage
- Depending on breach experts (legal, forensic, public relations)
- Data-packed website support
- Layered limits and available market capacity

CYBER LIABILITY INSURANCE



Green = 1st Party Benefits

CYBER INSURANCE - ONE APPROACH



The Insurer's "Breach Team" and negotiated rates are a valuable policy benefit

CYBER LIABILITY *CHANGING TIMES*

ERISA Advisory Council, 2011:

> ERISA does not directly address how employee benefit plans should protect PII of participants. Plans need to comply with many state disclosure laws because there are no overall federal issued guidelines. As state laws are developed in the area of privacy of financial data and PII, plan administrators will need to be cognizant of these rules and adjust their administrative practices accordingly.

ERISA Advisory Council, 2016:

> Plan Sponsors and fiduciaries should understand what cyber insurance does and does not provide and how it coordinates with other types of insurance coverage, so that they can appropriately consider whether to incorporate cyber insurance into their cyber risk management strategy.

Source: United States Department of Labor

APPLYING FOR CYBER INSURANCE

- Access how many records on hand and know how stored
- How many employees have access to data?
- Is there ongoing security training?
- Who's responsible for data security?
- Is there an incident response plan in place?
- In there an information security policy and how are violations handled?
- Are there contracts in place for 3rd parties who process, host or store sensitive information?
- What has the breach experience been and how handled?

"NO" ANSWERS COULD RESULT IN HIGHER PREMIUMS, NOT NECESSARILY DECLINATIONS

KEY TAKEAWAYS

In event of a cyberattack or similar incident, an entity:

- Must execute a response, implement mitigation procedures and contingency plans.
- Should report the crime to law enforcement agencies.
- May be required to report a breach to the OCR or similar regulatory body as soon as possible but not later than 60 days after discovery of a breach affecting 500 or more individuals.
- Noncompliance may result in a regulatory audit and/or require an entity or fund be required to pay fines and/or penalties.

THANK YOU!