2015 CLM Annual Conference

Palm Desert

Reducing Insureds' Data-Breach Risks and Damages

Presenters: Daniel Hecht, *Ironshore Insurance Company*
Hillard Sterling, *Winget, Spadafora & Schwartzberg, LLP*
Dan Twersky, *CNA Insurance*
Doug Worth, *Starwood Hotels & Resorts Worldwide, Inc.*

I. Assessing Pre-Breach Risk-Reduction Programs

A. Why Risk-Reduction Programs Are Important

It has become self-evident that businesses need to implement risk-reduction programs before they suffer data breaches or incidents. As with most other risks, preventive measures are critically important. Such measures may not succeed in avoiding intentional intrusions or negligent releases of data, but they may reduce the magnitude of the data losses as well as the potential exposure in damages, penalties, and reputational harm.

A strong risk-prevention program should have expansive technological, procedural, and legal components. Each business holding or transmitting sensitive data, for example, needs to undertake a comprehensive vulnerability assessment, implement technological security controls to anticipate and detect intrusions, build a solid risk-management program, craft a broad yet enterprise-specific incident-response plan, undertake realistic table-top exercises to test that plan, develop security policies that cover all potential points of intrusion, and train employees on those policies. And all of these components should pass muster under governing legal principles.

B. What Is (And Is Not) Typically Done

Before insuring cyber risks, most insurers have taken steps to assess that prospective insureds have comprehensive risk-reduction programs in place. The approaches, however, vary, and often miss the central question of whether the technological, procedural, and legal components, assuming they are in place, are effective or at least adequate.

For example, insurers often use checklists to determine that certain necessary risk-reduction components exist. These checklists, however, focus on whether certain risk-reduction components are present, not whether they are effective or even adequate.

Some insurers take additional steps and help insureds implement the requisite infrastructural protections, such as by web-hosting collections of precedents and

templates (of, for instance, incident-response plans and corporate policies). But, again, these precedents and templates are focused on helping insureds put the requisite components in place. The strength of a plan or policy comes from the extent to which it: (a) incorporates and accommodates the unique attributes of each business and its data, and (b) is communicated well to requisite personnel. Copying and pasting a plan or policy does not satisfy those critical predicates

The bottom line is that simply assessing or ensuring the existence of a risk-reduction program is necessary but not sufficient. A deficient risk-management program is just as bad, if not worse, than no program at all. An incident-response plan is worthless if the requisite personnel do not know what it says and how to follow it. And policies mean nothing if employees are not trained to satisfy them and sensitized to the dangers of non-compliance.

Accordingly, insurers and insureds should be focused on the deeper objective of strengthening data-breach risk-reduction programs. It is in both of their interests to do so. Insurers benefit by reduced exposure because insureds are armed with effective programs to reduce first-party and third-party damages caused by cyber breaches or incidents. And insureds reduce their risks of paying potentially large deductibles and suffering significant uninsured losses (not to mention uninsurable and potentially debilitating reputational harm).

II. Strengthening Pre-Breach Risk-Reduction Programs

A. Cyber-Risk Checkups

There are many ways that insurers and insureds can get to the heightened level of collaboration that is necessary to strengthen preventive measures against cyber risks. One approach is a "cyber-risk checkup," which focuses on improving the components of an insured's risk-reduction program, not simply noting or promoting their existence. This includes:

1. Preparing or Revising Policies

Strong data-security policies are the backbone of any breach-readiness plan. These policies should cover the multitude of ways that data is received, accessed, stored, transmitted, and used across the entire enterprise. Policies should cover internal and remote access, passwords, encryption, email usage and storage, mobile devices in and outside the workplace, network security, physical security, legal compliance (and its many facets), monitoring and logging, and many other areas depending on the business and the data it touches. Each business is unique in all of these respects, and the policies should be crafted and fine-tuned accordingly. Given the complexities, generic policies represent, at best, a start.

2. Preparing or Revising Incident-Response Plans

The same principles hold true for incident-response plans, which should be tailored to each business's particular structure, data, and legal duties. The plans are roadmaps for

acting quickly and effectively in the event of a potential breach and incident. As such, these plans should carefully delineate who gets involved and when, what steps must be taken to investigate and address the potential breach or incident (particularly in the critical early stages), and how information is to be communicated internally and externally. One central commonality is that all of these plans should involve outside counsel, as "breach coaches," to coordinate and quarterback the response and maximize the protection of information where appropriate under the attorney-client privilege and work-product doctrine, as discussed more fully below.

3. Undertaking Compliance Assessments

Breaches or incidents often are the impetus for businesses to focus closely on their legal exposure. By that time, however, the objective is to minimize or mitigate damages. It makes much more sense, for both insurers and insureds, to examine legal compliance before the damage is done through a data breach or incident. The analogy to other insured risks is probative. Better to focus on fire readiness before the fire, on health before the illness, on protective contractual provisions before a breach. And understanding the governing legal mandates, in turn, dictates the necessary specifics of other preventive measures, such as internal policies.

4. Developing or Improving Employee Training

A comprehensive risk-prevention program is only as strong as its weakest link, and deficient employee training may destroy an otherwise strong program. Employees need to be fully aware of data-security policies, procedures, and protocols. Awareness, though, is insufficient. Businesses should ensure that employees truly understand, and actually follow, policies aimed at protecting sensitive data. One recent trend is to test employees by distributing cleverly disguised emails that mimic phishing attacks, so that careless employees are identified and trained before they fall for pernicious hacking attempts in the real world.

5. Developing or Improving Table-Top Exercises

As with policies that are not communicated and followed, incident-response plans have little or no efficacy if they are not used and tested before a real breach or incident. Businesses should deploy realistic table-top exercises to rehearse the appropriate response to various foreseeable breaches or incidents. It is far preferable to identify and plugs gaps in the plan during a hypothetical exercise than to fall through them when it really counts.

6. Other Steps To Foster An Enterprise-Wide Security Culture

The underlying theme of all of these preventive measures is to foster a true security culture across the entire enterprise. There are many additional ways to do so. Corporate executives should be leading the charge, and they should be active and visible sponsors of preventive measures across the organization. Regular reminders of governing policies are helpful, particularly if done in creative ways. Consider measures that make corporate security interesting or even fun, such as contests and awards for the safest divisions or

departments. Meet and discuss these issues, and encourage active communication.

B. Utilizing the Attorney-Client Privilege and Work-Product Doctrine

Promptly upon discovering a potential data breach or incident, a critical first step is to initiate an investigation. The central objectives are to determine the nature and scope of the intrusion or loss, and to take tangible measures to stop or at least mitigate the resulting harm. The incident-response plan is the roadmap for meeting these objectives. Once these objectives are satisfied, additional investigatory measures will be necessary in order to develop and implement strengthened data protections, communicate with regulators and other interested constituencies, and prepare for potential litigation in administrative tribunals and courts.

Businesses need to protect their communications as much as possible during these investigations. It is in everyone's interests to communicate openly and often critically, and the incentives to do so are magnified exponentially if those communications are protected from disclosure to regulators and the outside world.

Outside counsel should be retained as "breach coaches" in order to protect associated communications, to the extent legally possible, under the attorney-client privilege and work- product doctrine. Courts generally recognize the privileged and protected nature of these communications when requested and/or directed by outside counsel for purposes of assessing legal risks and counseling on legal issues. By contrast, courts exhibit increased skepticism when adjudicating privilege assertions over communications that did not involve counsel, or that involved only in-house counsel (whose communications are more easily characterized as undertaken for business purposes rather than legal advice).

These principles also hold true for pre-breach risk-reduction programs. Outside counsel should be involved as "pre-breach coaches" to develop and implement measures aimed at reducing risks and damages from prospective breaches or incidents. Communications should occur at the direction or request of outside counsel, for purposes of assisting counsel to assess and address legal risks. Outside counsel should be central to the chain of written communications – hard-copy and electronic (including of course emails) – to ensure that those communications are appropriately labeled and managed to preempt prospective arguments that potentially applicable privileges or protections were waived.

C. Paying for Risk-Reduction Measures

Strengthening insureds' risk-reduction programs may be in everyone's interests, but less clear is the answer to the question of who pays for it. The expanding cyber-policy market is highly competitive, and insurers understandably do not want to add an additional layer of cost for themselves or their insureds. Strengthening risk-reduction measures as part of the underwriting or application processes, therefore, may seem to be a non-starter for many insurers.

However, the market may very well move in that direction as it matures. Although insurers may be reluctant to break from the competition and require affirmative risk-reduction measures as part of insuring cyber risks, the cost/benefit analysis may change

as data breaches multiply and the heightened costs of paying claims for unprepared insureds become clear. Similarly, insureds should become increasingly willing to assume additional costs as they become painfully familiar with the heightened risks and costs of not doing so – in deductibles, uninsured damages, and uninsurable losses including reputational and competitive harm.

Given those risks and costs, which are inevitable from a major breach, it would be rational for insureds to voluntarily assume the costs of strengthening their risk-reduction programs. Although the benefits may be difficult to calculate with specificity, there certainly are advantages and cost savings in being better prepared for a data breach or incident. Even if (and, for most, when) intrusions or losses occur, the damages invariably will be lower for businesses that are prepared. And the savings may be substantial for businesses that can tell a compelling story of preparedness when challenges come from prospective regulators or plaintiffs.