

Are you Covered?

Insurance for First-Party IT Risk

This article provides an overview of how a company can transfer first-party privacy risk.

Almost all companies face various IT systems failures, network security breaches, and privacy incident exposures (collectively “IT and Privacy Risk”) based on their daily business operations. It may surprise even the best managed company, however, just how much first-party IT and Privacy Risk it sometimes retains. For example, although during the course of engaging outside vendors, a company can sometimes offload some privacy risk to their vendors by way of contractual indemnification and insurance requirements. Such safeguards have no impact on risks caused by a company’s own employee negligence or wrongful conduct. And, what if the vendor’s choice of insurance policy is weak? Or, even going forward with a strong vendor insurance clause that is backed by an equally strong insurance policy, what about first-party loss exposures such as IT systems failure due to human error or reputation injury, internal forensic costs, or the expense of credit monitoring that results from a privacy breach?

First of all, major first-party privacy exposures can fit into two broad categories:

- **Commercial First-Party Loss** – Those true first-party losses derived from any privacy event, including reputation injury that is sustained by a company. Such events may involve a systems failure due to an employee’s error unrelated to a network security breach or a systems failure related to third-party malicious code used to obtain sensitive data.¹ In any scenario, although there is no pending claim, the company may incur significant expense or revenue loss as a result of the event.
- **Regulatory First-Party Loss** – Those defense expenses incurred when defending a regulatory action based on a privacy breach as well as those fines and penalties levied by a governmental entity. Such quasi-liability/quasi-first party expenses are routinely excluded from most standard policies and depending on the wording insurance policies covering such loss may be deemed as void against public policy.

These potentially significant exposures are left unchecked and unprotected under most General Liability policies. Similarly, an Errors & Omissions policy is of little value

given that it will provide an express trigger that ties only to claims brought against the insured. As a result, first-party IT and Privacy Risk is generally either retained, transferred to others who may actually have caused the loss, or transferred to a specialty insurer.

What to Look for in a First-Party Policy

When evaluating policies that provide first-party privacy coverage, it is especially important to have a very broad trigger for coverage. For example, the policy should include triggers for the unauthorized use or access of a computer system such as a computer attack; transmission or receipt of malicious code; denial of service attacks; social engineering incidents such as phishing; and any unauthorized disclosure of confidential personal or corporate data. There should also be no exclusion for the intentional, dishonest, fraudulent or criminal acts of the company’s agents, employees, or independent contractors. Moreover, the coverage should extend out to the defense of a regulatory action brought as a result of a data breach or privacy incident. And, as discussed further below, coverage should also extend out to the following expenses related to a breach incident: breach notification costs, credit monitoring, forensics, and call center expenses.

What happens if a data thief or rogue employee causes your network to go down? There are several markets that provide “property-like” coverage for business interruption and extra expenses incurred when a company’s computer network is down. Such first-party coverage can be triggered by a data thief who has caused damage to a network or is caused by a company that is forced to shut key components of its system out of safety concerns. The key differentiator between this sort of coverage and a typical property policy is that there is no requirement that there be physical damage to property in order to obtain coverage. Even without any accompanying physical damage, costs to restore data and get a business up and running again can be significant – and completely uninsured under your typical property policy. Some policies also provide coverage to “resecure” privacy data under the insured’s control.

Coverage can be purchased as well that provides reimbursement of lost income due to a systems breach. There is also coverage that can be obtained that provides for lost income reimbursement even if the system is down solely due to human error unrelated to any breach of security. One area where the insurers differ on business interruption coverage

**Are you tired of losing
sleep over system failures
and non-compliance issues?**



**Sleep better with IAITAM-
Endorsed Insurance Products**



For more information please contact info@iaitam.org

turns on how lost income is calculated. Accordingly, the ultimate goal when negotiating such deals is to ensure the method for calculating lost profits remains as objective and clear as possible. The more work done up front will obviously reduce the workload when a claim is tendered for payment.

Another form of coverage that has somewhat of a standard lines analogue is the “cyber-extortion” coverage that some insurers can provide. Unlike with a typical Kidnap & Ransom policy, however, this coverage is not for a person but rather for a computer system. For example, the “cyber-extortion” coverage will allow for payment of an extortion demand made which threatens to divulge or utilize data residing on the insured’s network or to initiate a denial of service attack.

Coverage for the Costs to Respond to a Privacy Incident

In order to deal with the potential reputation harm that a privacy incident can engender, a company is well advised to also purchase the crisis management option available under certain policies. This coverage allows the insured to retain and use a crisis management firm specializing in managing the aftermath of a privacy incident. Given that even the smartest companies can act like deer caught in the headlights when confronted with a privacy incident, having access to a PR firm that has actually handled several privacy incidents is of major help. This insurance coverage not only provides access to such well-qualified firms, it also funds their use.

Breach notification costs can also be significant. Since California implemented its breach notification law in 2003, 42 other states, the District of Columbia, and Puerto Rico have followed suit – with the Federal Government soon poised to enter into the fray. Given that compliance with these notification laws is driven by legal counsel, legal expenses related to a privacy incident can quickly mount. Moreover, depending on the size of the notification pool, notification costs themselves may justify transfer via an insurance policy. Thankfully, privacy breach notification costs are reimbursable with policies available on the market. When notifying a client or employee of a privacy breach incident, companies also generally like to include the fact that credit monitoring will be provided free of charge. Whether the credit monitoring is ultimately tri-bureau or single bureau or for one year or two years, such significant costs can be covered under most privacy policies. And, even if a company already has a call center operation, it is important that the policy includes providing broad enough coverage to reimburse for such expense – whether or not it is outsourced.

Other Considerations

When choosing first-party coverages, it may also be relevant to focus on how a company is impacted by contracts it has with third parties. For example, a large retailer may have significant contractual exposure should it violate the



Payment Card Industry Data Security Standards (PCI DSS). Although contract breach damages are not commonly provided for in an insurance policy, some insurance markets may be willing to provide PCI DSS penalty coverage – with or without a privacy incident to otherwise trigger coverage.

It is also important for those looking at first-party insurance to be current with their business continuity (BC) and disaster recovery (DR) plans. When underwriting these first-party policies, some insurers will want to make sure the network security, privacy, DR, and BC procedures put in place at the time of the insurance application will stay in place during the entire time the policy is in force. Any deviation that lessens security or adversely impacts the business may lead to a loss in coverage. The best means to ensure compliance with this sort of requirement will be to have the right personnel make sure the completed application and assessments are accurate.

Finally, although these new policies afford companies for the first time the luxury of transferring certain high-exposure first-party risk, they have still been coming down in price due to the overall soft Property & Casualty insurance market. When considering how to take advantage of the current favorable environment, the coverage enhancements able to be negotiated should always remain of paramount concern. After all, when the insurance market hardens again – and it will, it will be much more difficult for insurers to remove negotiated coverages than it will be to raise premium.

¹⁾ Although most press accounts focus on network security failure, an Economist Intelligence Unit survey conducted several years ago revealed that more than half of the European companies polled had suffered during the previous twelve months significant financial damage as a result of IT system failure caused by employees or contractors. Given that such failures had nothing to do with a network security breach event; they would not trigger a traditional “cyber” policy; but rather, would only trigger a “systems failure” policy.

Paul Paray, Esq.
*Senior Vice President
 Hilb Rogal & Hobbs of
 New York, LLC*

*Copyright ©2008 Hilb Rogal & Hobbs of New York, LLC
 All Rights Reserved*