Laurie Schwarz, Senior Vice President, Global Technology and Privacy Practice, shares insights on network security and privacy liability coverage.

Cyber exposure is characterized as companies with “data” exposure from a network security and privacy liability standpoint, whether as a data owner or data vendor with a service offering in connection with it. For the purposes of this report, I am speaking about companies that have a predominantly cyber exposure, but with media and technology exposure as well.

Traditional Network Security and Privacy Liability Coverage

Capacity remains consistent to slightly growing for traditional network security and privacy liability coverage. There are excess markets wanting to move down in the program. There are new markets within the past year coming into London that tend to be MGA driven with Lloyd’s paper, and they are often trying to one-up each other when it comes to sublimits.

Markets remain fragmented for sublimits for first-party privacy expenses, which include notification costs incurred when complying with data privacy notification laws, investigation costs, or crisis management expenses. Some markets, particularly out of...

Coverage has been fairly consistent. When incumbents try to drive rates other markets are willing to step in and be competitive on price.
London but a few out of the U.S., provide full limits. For smaller mid-market firms, the marketplace offers a per-person or dollar amount outside of the liability limit. If the market will only offer a sublimit, then those purchasing multiple layers of coverage will have excess layers drop down on the sublimits on a follow-form basis to drive limit adequacy for the coverage.

The costs—claims expenses, damages, and consumer redress funds and fines—associated with a privacy regulatory proceedings are generally covered as a sublimit under privacy liability. Currently, the market ranges from full to partial limits, and it continues to respond to inquiry, investigation, or proceedings arising from an alleged wrongful act.

Given the diversity of tech clients, in terms of their services and products, the competitive pressure from other markets will vary based on the company’s risk profile. For example, payment processors are finding it to be a challenging market given the recent amendments to merchant service agreements in the payment card industry.

First-Party Network/Business Interruption Extra Expense

There has been some movement in this area toward providing the full limit, even if a third-party vendor causes the degradation or the outage of service. This was not the case a year or two ago. Additionally, markets are more willing to consider broadening the trigger for coverage to include administrative errors, whereas before, it only covered malicious events.

Reputational Harm

In my opinion, reputational harm is the greatest area of development in this space. Previously, markets were providing expense reimbursement for public relations and messaging after a breach, but most companies didn’t find that meaningful because they tended to handle the messaging internally and didn’t go through a third party.

There are more markets out of London wanting to provide coverage for the loss of revenue and extra expense around reputational harm. Previously, the market capacity for this risk was limited. This coverage tends to be very tailored to the needs and concerns of the client, whether the peril is a data breach, a supplier issue, a whistleblower, a spokesperson, etc. This is an area of great interest for the larger companies with known brands, and is an area to watch for growth in 2013 and 2014.

The technology E&O marketplace is also firming with some markets driving rate increases.
Intellectual Property Theft

Intellectual property theft is a hot topic, because it is not addressed well in the marketplace. However, espionage is not new. For example, McAfee, in its report Operation Aurora, or more recently, Operation Shady Rat, has been writing about companies among various industry verticals having been breached for months, maybe years unbeknownst to them, while their IP is going out the back door. This is problematic because some big-name companies have fallen victim to this, and concern is growing among their peers. The marketplace is still finding its way in this regard, trying to determine:

1. How to value the intellectual property.
2. How to build insurance around either the loss in value of their IP or the loss in revenue; it's a topic we are talking about today, inside and outside the insurance industry to help insurers come up with a way to value and measure the loss in value of IP or future revenue.

Industry Sectors

The utility market has seen some growth in this area, with more utilities actively looking to purchase coverage as threats expand against critical infrastructure. This is an area that is getting attention by the current administration with a view of federal legislation on the horizon for 2014-2015 stemming from the Cyber Security Executive Order issued earlier this year. As more consumers get connected to the grid, and the multitude of systems that can access customer data and impact loss of revenue and extra expense grows, the marketplace is looking to deal with the complexities between infrastructure and traditional corporate networks. This is an emerging area, and currently Lloyd's is leading in this area developing a product addressing the loss of income and asset damage from SCADA systems.