Demystifying cyber insurance coverage

Clearing obstacles in a promising but problematic growth market

Deloitte. University Press

The threat of a cyberattack is gaining widespread attention, given the rise in highly publicized breaches and identity theft incidents. While the cyber insurance market is expected to double or triple over the next few years, it has been slow to develop.[1]

Only 29% of US businesses have cyber coverage

Only 40% of Fortune 500 are covered

Even those with coverage are often underinsured

Obstacles to growth: Why isn't the cyber insurance market expanding more quickly?

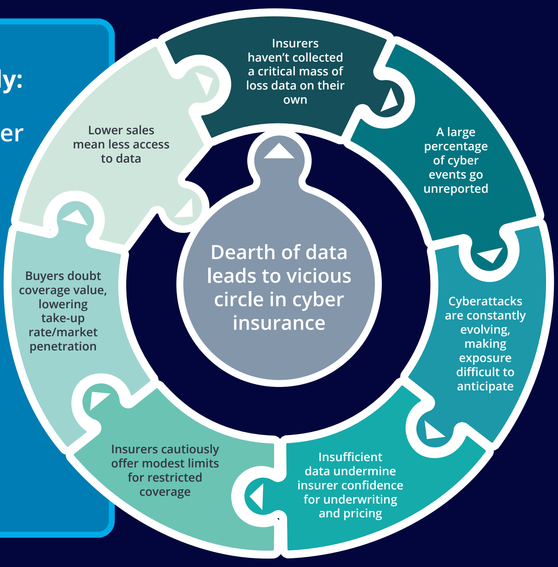
Insurer's perspective

- Dearth of data
- Cyber attacks keep evolving
- Potential catastrophic accumulation
- Tunnel vision in coverages offered

Consumer's perspective

- Buyers often don't understand cyber risks or their insurance options
- Cyber risk is spread over a wide range of coverages
- Cyber policies lack standardization
- The legal landscape remains in flux

Data in short supply: The vicious cycle of cyber insurance



Getting over the hump: Top strategies to overcome obstacles

Data-challenged insurers could buy time with alternative approaches, including:

- Developing risk-informed models
- Leveraging insurer's internal cyber-security expertise
- Adopting a customer segmentation approach, specializing in certain industries
- Focusing on specific areas of exposure (e.g., data breaches, denial of service, cloud, domain name servers)

Insurers could go beyond risk-transfer and offer holistic cyber risk management programs to:

- Support/become the client's cyber risk manager
- Provide risk prevention/recovery services
- Leverage insurer's cyber loss control program for risk alerts

Insurers should pave the way for growth by:

- Spreading risk with layers and reinsurance to avoid aggregation issues
- Raising risk awareness through education efforts, directly and via agents/brokers
- Standardizing policy language to develop a common lexicon, clear up buyer confusion, and avoid claim disputes

The risk of delay: Bigger buyers have other options

Insurers that don't crack the code soon could lose out to alternative risk-transfer vehicles, such as:

- Accessing the reinsurance market directly by forming a captive
- Joining together with similar companies to self-insure via risk retention groups
- Tapping the securities markets by issuing cyber bonds to investors

Stepping up: Where should insurers start?

Before entering or expanding their presence in this market, insurers should ask themselves:

1. Can we assess this risk with our current resources? If not, should we consider purchasing external data or third-party models to support underwriting and pricing systems?
2. How might we work within the industry to standardize our policy language, while still leaving room to differentiate products and services?
3. How can we leverage our own experience and expertise in managing cyber risk to support our clients?

[1] Sam Friedman and Adam Thomas, *Demystifying cyber insurance coverage*, Deloitte University Press, February 23, 2017, p. 2.