UT LAW CLE THE UNIVERSITY OF TEXAS SCHOOL OF LAW

PRESENTED AT

3rd Annual Government Enforcement Institute

September 29-30, 2016
Houston, Texas

Cybersecurity for Business Infrastructure

Mark L. Krotoski

CYBER INSURANCE

Mark L. Krotoski and Jeffrey S. Raskin

Cyber Insurance Coverage Considerations:
Determining Whether You Have the Coverage You Need

Cyber insurance is often recommended to protect against data breaches, business interruption, network damage, and related incidents. Where coverage applies, cyber insurance can mitigate substantial losses after a significant data incident or compromise occurs.

One senior Department of Treasury official compared cyber insurance to flood insurance in considering cyber threat protections in the banking industry:

> Cyber insurance cannot protect your institutions from a cyber-incident any more than flood insurance can save your house from a storm surge or D&O [Directors & Officers liability] insurance can prevent a lawsuit. But what cyber risk insurance can do is provide some measure of financial support in case of a data breach or cyber incident. And, significantly cyber risk insurance and the associated underwriting processes can also help bolster your other cybersecurity controls. Qualifying for cyber risk insurance can provide useful information for assessing your bank's risk level and identifying cybersecurity tools and best practices that you may be lacking.[1]

Cyber insurance coverage raises other issues with regulators. For example, in October 2011, the Division of Corporation Finance of the Securities and Exchange Commission provided guidance concerning cybersecurity risks and cyber incidents. One disclosure factor for public companies to consider includes a "[d]escription of relevant insurance coverage."[1] In recent cybersecurity examinations of registered broker-dealers and registered investment advisers, the Office of Compliance Inspections and Examinations asked whether "the Firm maintain[s] insurance that specifically covers losses and expenses attributable to cybersecurity incidents?"[2]

The cyber insurance field is new and emerging. While cyber insurance is an important factor for companies to consider as part of an overall cybersecurity protection strategy, the coverage and terms vary significantly. Buyers should be careful that they have the coverage they need.

Cyber insurance coverage raises a host of issues. This summary highlights some coverage issues that may be appropriate to consider.

[1] Division of Corporation Finance, Securities and Exchange Commission, CF Disclosure Guidance: Topic No. 2, Cybersecurity (Oct. 13, 2011), *available at* https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[2] Office of Compliance Inspections and Examinations, Cybersecurity Examination Sweep Summary (Feb. 3, 2015), *available at* http://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf.

Companies will need to purchase third-party and first-party "cyber" coverage

Third-Party Coverage

- Traditional General liability (GL) and Directors & Officers (D & O) insurance policies likely will *not* cover privacy breaches in the future as insurers develop new "cyber insurance" products specifically tailored for this purpose.
  - Many cyber breaches will be deemed *not* to be within the insuring agreements of GL and D & O policies.
  - Insurers also will add broad exclusions precluding coverage for cyber breaches.
- Companies will need to purchase separate "policies," or add-on coverage, to protect them, their directors and their officers from liability resulting from privacy breaches.
- Specialty "cyber insurance" products should be tailored to work seamlessly and consistently with GL coverage to avoid coverage gaps.

First-Party Coverage

- Coverage should also be purchased to cover the expense of remedying system breaches, the expenses of replacing damaged hardware and recreating lost data, the lost revenue resulting from the loss of use of a system during and following a breach, etc.
- This can sometimes be included as an additional benefit in third-party liability policies.

Cyber insurance is largely un-regulated at this time

- Policies are not standardized.
- There are numerous different products, with different terms, conditions, definitions and coverage afforded by the insurers.
- This coverage is largely un-tested by the courts, and there is scant guiding authority as to how the coverage applies, or does not apply, in the real world.

One size does not fit all

- A company in the business of handling and maintaining personal data will need different coverage than a retailer that handles and maintains personal data incidentally as part of its business.
- The un-regulated and non-standardized nature of cyber insurance means that substantial opportunities exist to design policies for particular risks and to negotiate favorable coverage terms and appropriate limits of liability.
- Coverage becomes relatively less expensive at higher levels of coverage. There is no reason not to be fully covered for a potential cyber breach.
- Coverage can be obtained to cover the costs of notifying persons whose data may have been compromised, for hiring outside forensic analysts, and for the costs of hiring external crisis mangers. These costs can often be reimbursed "in addition to" the limits of liability that apply to third-party claims and lawsuits.

International coverage

- Cyber breaches are not confined by international boundaries. Hackers can strike from anywhere.
- Even small, local companies should make certain that "cyber insurance" covers breaches from wherever they originate.