While the risks posed by data breaches are now widely recognized, effective management of the risk is lagging. Statistics indicate that concern about data breaches is up, yet half of all businesses have no plans to dedicate more resources to avert these perils.

The purchase of dedicated cyberinsurance products appears to be on the rise, but many in the insurance brokerage community indicate that the marketplace is not yet as robust as one would expect given the staggering scope of recent data breaches and the ensuing headlines.

Figuring out what kind of insurance is needed to respond effectively to cyberclaims is challenging. Recent history teaches that the losses occasioned by cybersecurity breaches are not always predictable. The Sony Pictures breach is a prime example, as it imperiled or implicated in one fell swoop proprietary and intellectual property, employee personal information, sensitive management communications, reputation/goodwill, extortion, threats of bodily injury and business income. Now that hackers are extending the playing field of targeted data beyond the familiar categories of customer credit card numbers, addresses and health-related data, risk managers need to re-prioritize certain protections (including insurance protection) that used to be lower down on the shopping list.

Further widening the scope of cyberclaims, D&O insurance came into the picture last year after data breaches spurred derivative lawsuits against company officers and directors. While cyberinsurance products are finally registering on the radar of senior corporate executives, D&O insurance policies remain nearest and dearest to directors’ and officers’ hearts. It is therefore essential that D&O insurance respond to suits targeting company managers and directors that have their genesis in data breaches.

Purchasing adequate insurance coverage for technology-related insurance claims is challenging, as products lack uniformity and the claims history is thin. Following the tips below will improve the chances of recovery from stand-alone cyber and D&O insurance policies.

1. Pursue Clarity: Buy an insurance policy that you can actually understand. Unfortunately, many stand-alone cyberinsurance policies are virtually incomprehensible. Since there is not a lot of uniformity of product right now in the marketplace, many policies are confusing and densely written, making it hard to determine the scope of actual protection provided. Comparison shop with a good insurance broker at your side to help you find the best forms. Once you have a good, comprehensible form to work with, the insurance company will often endorse it to provide protection that is better tailored to your needs if you know what to ask for.

2. Cover the Evolving Risk: Continuously monitor trends in computer hacks and data breaches. Remember that data breaches can still occur the old-fashioned way, through theft of sensitive hard-copy documents, as well as in cutting-edge ways not currently imagined. Your insurance policy needs to match the underlying exposure.

3. Cover Time-Element Losses: Business income coverage and reputational damage coverage take on added importance in the wake of recent hacking events. While a slew of insurance companies have offered cybercoverage for business income losses and reputational damage for several years, that coverage was not nearly as coveted as class action privacy litigation coverage, breach notification costs or regulatory proceedings coverage. Now, the reality that a breach can imperil the very core of the policyholder’s ability to continue business operations takes on much greater import for risk management objectives. As such, consider insurance coverage that pays...
time-element claims resulting from reputa-
tional damage and business interruptions,
including ones that partially interfere with
business income.

4 Seek Retroactive Dates: Push for retroac-
tive coverage whenever possible. Many
insurance companies want to provide in-
surance protection only from the date that
the first policy they sold you incepts. The
problem is that some cyberthreats occur
well before the policyholder actually learns of
them. Computer forensic specialists will
tell you that computer hackers can intrude
into a computer system weeks, months and
even years before the policyholder becomes
aware of the threat.

If you purchase insurance coverage with
a retroactive date that pre-dates the policy
period, your cyberinsurance company may
ask you to provide a warranty letter. If
you provide one, make sure it is carefully
written and ensure that you do your due
diligence in reaching out to other depart-
ments and employees within the company
to ensure that your representations are fair.

5 Avoid Breach of Contract and Warranty
Exclusions: Resist efforts to include
breach of contract exclusions in your cover-
age. These provisions should be obsolete in
an era in which so many policyholders do
business pursuant to a contract (whether
with customers, credit card companies, fi-
nancial institutions, etc.). These exclusions
are used all the time by some insurance
companies to challenge insurance claims.
While some recent court decisions have
curtailed this use, it is best not to have the
fight in the first place.

6 Avoid Cybersecurity Reasonableness
Clauses: Resist insurance company
efforts to include exclusions, warranties,
representations or “conditions” in insur-
ance policies concerning the soundness or
reasonableness of the policyholder’s data
security efforts/protocol. These clauses
are a recipe for disputes on potentially
every security incident. Given the pace
of technological innovation, almost every
security step can be second-guessed with
the benefit of 20-20 hindsight. Is it safe to
log onto a secure network from your luxury
hotel room using the hotel’s wifi? The
answer depends upon many factors that are
difficult to pinpoint, including the exact
point in time in which attitudes collectively
begin to change. Such a question is bound
to end in dispute if the cyberclaim is big
enough.

7 Preserve D&O Insurance Coverage
for Cyberclaims: Keep your directors
and officers (D&O) insurance program
( primary, excess, Side A, etc.) clean from
any cyber-related exclusions or sublimits.
Management will be highly concerned
with any argued “gap” in coverage should
a cyberevent ensue and D&O coverage be
contested on the basis of an exclusion or
limitation for suits where cyber may be the
underlying cause or context of the claim.

8 Be Thorough When Filling Out Cyberin-
surance Policy and D&O Policy Ap-
lications: Complete insurance applications
carefully and gather information from
other business units where necessary when
answering questions. Even if an insurance
company must pay a claim under the plain
terms of the insurance policy, cover-
age may still be contested, under certain
circumstances, on grounds that application
questions were not correctly answered.

Do not give the insurance company this
opportunity.

9 Remember That Cyberbreaches Happen
Off-line Too: Make sure your cyber-
specific coverage protects losses involving
mobile devices, home offices, data that is
off-line at the time security is breached and
devices that may not be owned by the poli-
cyholder. A lost flash drive containing gi-
gabytes of information can lead to a breach
and possibly an expensive one. Make sure
your insurance coverage is available for
such a scenario – even where the device is
not actively connected to a network when
the data breach occurs.

10 Cover Cloud and Third-Party Vendors:
Make sure that your cyber-specific
coverage protects against losses where oth-
ers manage, transmit or host data for your
company. Insurance coverage is available
for cloud computing and instances where
data is handled, managed or outsourced to
a third party. Going back to point num-
ber one above, however, not all insurance
policies are created equal, and there are
cyberinsurance forms that on their face ap-
ppear not to provide express protection for
cloud-like scenarios. Most of these policies
can be modified to extend such protection
– if requested.

A static assessment of data security
risk management will not work in most
instances, given the rapid pace of change
in this area. Be vigilant and adaptable in
managing the security risk. Work with
your colleagues in other departments to
reduce risk where you can – and secure the
best insurance your company can afford
to protect against losses stemming from
cyber-related perils.