AMERICANS HAVE LEARNED TO LIVE WITH BIG RISKS—including, for the past few years, losses from major cyberattacks. With news of major data breaches breaking almost daily, the public is growing numb and, to a certain extent, so are the businesses that must absorb the cost of enhanced cybersecurity.

These companies are bombarded with Armageddon-like scenarios involving large security breaches, and urged to model and insure against increasingly complex data losses. This has created demand for more comprehensive cyberinsurance products, and insurance companies have hurried to meet the demand. Cyber is the new insurance gold rush.

But past insurance gold rushes have ended badly for underwriters that ignored their risk modelers and the inevitability of losses from cyclical perils, then sold policies aggressively to get premiums in the door. Will insurance history repeat itself with cyberrisk?

by DAVID E. WOOD
ARE WE THINKING BIG ENOUGH?

There is evidence that what insurance markets now regard as a catastrophic cyberloss may actually be a warm-up for the main event. Recently, the federal government and some of the nation’s biggest companies have begun working in concert to identify, measure and protect against a mega-cyberloss—one so big that it impacts national security and causes the stock market to falter or worse. The American business and government sectors have done a great deal of work to better understand and guard against the economic vulnerabilities created by cyberattacks.

At least one insurer says it can model the risk of a mega-cyberloss based on prior data breaches. But what if the risk of a massive cyberassault cannot be effectively modeled based on existing data? Insurers would then be forced to compete over cyberinsurance premiums more or less in the dark.

In the wake of a huge natural disaster, insurers often withdraw from writing property policies, or threaten to withdraw in an effort to gain government aid. For example, following Hurricane Katrina in 2005, State Farm stopped writing commercial and homeowners policies in Mississippi, citing the state’s “current legal and political environment.” This was a tacit admission that insurance companies incorrectly modeled risk, failed to mitigate risk through diversification and/or transfer to reinsurers, or did not heed their own risk modeling in pricing policies.

If history repeats itself and insurers are as unprepared for a mega-cyberattack as some property insurance companies were unprepared for Katrina, then the sheer magnitude of such an attack—thought to vastly exceed the cost of any natural disaster in history—could do far more than merely increase the cost and decrease the availability of insurance going forward. Unprepared insurers could be financially unable, or far less willing, to pay claims.

Shareholders are increasingly averse to bearing insurable risks. The Securities and Exchange Commission has made clear its expectation that public companies must fully disclose their exposure to cyberloss and the measures they take to mitigate it, including insurance. Against this backdrop, should a massive cyberattack ever call into question major insurance companies’ willingness and ability to promptly pay claims, shareholders could take out their frustration on the corporate policyholders who are victims of the assault. Thus, the key question is whether the insurance industry is ready for the “Big One”—the cyber-event so catastrophic and crippling that it broadly threatens the American economy.

PREPARING FOR CYBERWAR

The Government Accountability Office warned in its 2013 High Risk Report that cybersecurity incidents affecting computer systems and networks throughout the nation continue to rise. As a result, the risk generating the most concern among businesses and government today is an attack on critical infrastructure. In Executive Order 13636, the White House defined “critical infrastructure” as “systems and assets so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on national security, economic security, public health or safety, or any combination of those matters.” In February 2014, the National Institute of Standards and Technology (NIST) released a risk-modeling program putting this Executive Order’s stated objectives into action in order to help companies assess and set their risk tolerance for cyberattacks. In January 2015, the Obama administration proposed legislation that would encourage companies to share cyberthreat information with the Department of Homeland Security, which would, in turn, be charged with disseminating that information to other companies and federal agencies.

The defense industry and agencies of the federal government that are responsible for military threat analysis warn of an imminent “cyber Pearl Harbor” in which a sneak attack on some strategically critical pillar of U.S. infrastructure causes a series of cascading losses throughout the economy. The U.S.
Department of Energy is developing what it calls a Cyber Attack Risk Inference Model (CARIM) for energy companies with operations of particular strategic importance, such as utilities, the bulk electric power grid, and oil and gas supply and distribution.

The non-defense private sector is also taking steps to improve readiness. In the financial services industry, several large banks have conducted exercises with evocative names like Quantum Dawn 2 and Systemic Strike, that simulate a large-scale cyber-assault to test the security controls of financial institutions. A February 2014 Bipartisan Policy Center report urged energy companies to cooperate by creating an industry-led body to detect cyberthreats to the electric grid. The American Water Works Association’s 2014 “Process Control System Security Guidance for the Water Sector” recommended a set of best practices to protect water utilities from cyberattacks.

Trade associations representing industries classified as critical infrastructure in Executive Order 13636 are warning their constituents of the heightened risk of a mega-cyberattack. For example, the North American Electric Reliability Corporation reported in 2012 that the U.S. power grid remains susceptible to cyberinfiltration, despite substantial government investment in securing it. A widespread assault on the electric grid could suddenly shut down the banking system, bringing the economy to a grinding halt and causing a plunge in the stock market.

This sense of urgency is felt by chief technology officers and risk managers alike. In a November 2014 survey by the Association of Financial Professionals, 70% of respondents rated the level of priority their organizations placed on cybersecurity a 4 or 5 on a five-point scale. More than two-thirds said their organization had updated its cybersecurity response plan within the past year.

**THE INSURANCE INDUSTRY RESPONSE**

Virtually all domestic companies writing commercial insurance have joined the cyber gold rush, and corporate policyholders have a range of options. The best policy forms have a wide variety of features, such as, under first-party policies, coverage for crisis management in the wake of a data breach, the cost of notifying customers and providing credit monitoring services, and ransoms paid to stop a cyberattack. Under third-party policies, covered losses can include fines and penalties due to breach of payment card industry data security standards, and unfair competition and intellectual property infringement liability surrounding the gathering and protecting of customer data.

Demand for these insurance products is on the rise. According to a Marsh report from April 2014, cyberinsurance purchases across all industries rose by 21% in 2013, and the buying trend appeared to be accelerating.

Some experts also believe that cyberinsurance is underpriced globally. This may be because the threat of cyberattack is relatively new, as is the pervasiveness of the internet itself. Only in the past several years have government and industry leaders begun to sound the alarm about the risks of a catastrophic cyberattack.

Further, catastrophes are harder to model than routine perils—and a peril that has not happened is even more difficult. Underwriting and pricing for any insurance policy must include an understanding of historical loss data and a quantification of the risk to be insured. If a mega-cyberattack has never occurred, how can the underwriter understand the history of this risk and adequately quantify it for pricing purposes?

Normative underwriting standards to assess prospective policyholders’ preventive efforts are also undeveloped or unavailable. Good data security is a constantly moving target, and what was up-to-date security yesterday is often out-of-date today. Because they are thus unable to assess the long-term strength of data security, insurers are pricing cyberrisk without a fixed baseline.

Just as dangerous as the disassociation of risk modeling from pricing is the over-concentration of risk in a particular market. For instance, California deregulated rates for workers compensation insurance in 1995. A free-for-all followed as a number of insurers competed for market share. This resulted in significant underpricing of risk and, ultimately, the insolvency of several companies that were heavily concentrated in the California workers compensation market.

**WILL INSURERS BE ABLE TO PAY CLAIMS?**

There is no question that a mega-cyberattack is coming. Therefore, it is fair to ask:

1. Will the business and government sectors have adequately planned for this catastrophe to minimize its financial impact on the economy?
2. If the national cost of current cyberattacks is as much as $160 billion, as one analyst projects, will the private sector’s net worth be sufficient to withstand the loss from a mega-event, and more importantly, prevent equity markets from collapsing?
3. Will insurance companies withdraw from selling cyberinsurance, or dramatically hike premiums and lower limits while raising retentions, indicating that they did not accurately model and price this catastrophic risk? Will they be called to testify before Congress, as property insurers were after Hurricane Katrina, to assure customers of their willingness and ability to pay claims? How will they respond?

To improve insurers’ underwriting of this risk and boost confidence among corporate policyholders that these claims will be paid, several things must take place:
First, while good work is being done by industry trade
groups, federal agencies and individual companies to measure
and plan for a mega-cyberattack, this work suffers from a lack
of cross-industry and cross-sector coordination. In Executive
Order 13656, the White House called for a public-private part-
nership to achieve this. The defense industry and the federal
government agencies it serves appear to be ahead of the curve.
Their coordinated efforts can and should be replicated in the
larger economy.

Second, while much has been done to improve the public
and private sectors’ position in the arms race with cybercrimi-
nals, this effort must be continual. The public needs to feel,
credibly, that it is a step ahead of the bad guys, rather than a
step behind.

Finally, there is an acute need for development of agreed-
upon data security standards to guide companies in their prep-
aration for the Big One, and to which insurance underwrit-
ers can refer in evaluating risk and pricing policies. Although
the NIST Framework for Improving Critical Infrastructure
Cybersecurity “uses risk management processes to enable orga-
nizations to inform and prioritize decisions regarding cyberse-
curity,” it is not a risk management process and does not actu-
ally establish any security guidelines.

If Congress were more effective at bipartisan problem-solv-
ing, it could address this need by appointing a special com-
mission to hear evidence from security experts, risk managers
and insurance underwriters to generate a set of best practices
for measuring and protecting against the risk of a catastrophic
cyberattack affecting critical infrastructure.

The worst-case scenario, when the Big One happens, is that
insurers will disengage from their corporate policyholders just as
the wave of catastrophic claims breaks over insurance markets.
When this catastrophe happens, policyholders and their insurers
must re-engage at a deeper level to work through the aftermath
of a disaster. But this kind of re-engagement is unlikely to happen
without better underwriting and pricing of cyberinsurance, cou-
pled with the best possible policy forms that minimize insurance
companies’ ability to raise technical coverage defenses. Without
these important controls, it will be difficult for corporate poli-
cyholders to remain confident that, when the inevitable mega-
cyberattack happens, the insurance industry will be ready for
it—and willing to pay the enormous claims that will undoubt-
edly result.

David E. Wood is a senior shareholder in the Ventura, Califor-
nia, office of law firm
Anderson Kill and co-chairs the firm’s cyber insurance recovery group.