# Can Your Clients' Existing Property Policies Protect Their Digital Assets?

*Traditional property insurance programs may not cover cyber risks such as computer viruses, denial of service attacks and confidential information theft. By excluding damage to intangible property, such programs leave companies vulnerable in the event of a major computer attack.*

*Risk managers and CFOs would agree that information on their corporate networks represents a significant portion of the assets that appear on a corporation's balance sheet. Trade secrets, proprietary software systems and databases are just a few of these intangible assets.*

*Despite a company's best efforts to improve computer security, hackers, cyber thieves and cyber terrorists continue to successfully break into networks and cause catastrophic financial losses. In many cases, such losses are not covered by insurance.*

*In order to protect digital assets and a company's bottom line, specialized insurance solutions are required. Recognizing the need to provide coverage for certain types of cyber risk, the Lexington Insurance Company created* ***LexCyberSecure℠***.

## LexCyberSecure℠

Lexington Insurance Company, one of the world's leading property and casualty companies, can provide a computer attack coverage endorsement that will enable insureds to obtain coverage for certain losses suffered due to a failure of their computer security. Coverage in the endorsement includes information asset protection, network business interruption and cyber extortion.

### Information Asset Protection

- Provides coverage for property losses involving data, computer systems resources and information assets, such as credit card numbers and customer information, resulting from a failure of network security caused by a computer attack so that such information assets can be restored or recreated.

### Network Business Interruption

- Provides coverage for business interruption losses arising from the interruption or suspension of your client's computer network due to a failure of your client's network security caused by a computer attack. This coverage includes business income and extra expense, as well as funds for forensic and investigative services and contingent dependent business interruption.

### Cyber Extortion

- Provides coverage for extortion threats related to intentional computer attacks. Includes coverage for both the investigation and settlement of an extortion threat against the insured.

### Additional Benefits

- On-site ISO 17799 security audit for qualifying applicants at no additional cost.
- Coverage from a financially superior, highly rated insurance company.
- For qualified applicants, the limits of liability for each coverage can be up to $25 million subject to an aggregate limit of liability for all coverages up to $25 million. Other sublimits may apply to certain coverages.

*continued on back*

## The Danger Is Very Real

Some examples of these dangers include:

**— U.S. Bank and Airline**

*Loss of Electronic Data and Business Interruption*

Over 160,000 computers worldwide were hit by the Slammer worm, impairing key systems in the U.S. government and private sector. A major U.S. bank reported that most of its 13,000 ATMs could not process customer transactions for one day. At the same time, a major airline reported flight delays and cancellations after the "worm" overwhelmed online ticketing systems and electronic kiosks.[1]

**— Fortune 500 Technology Company**

*Employee Breach of Security*

A former employee sabotaged performance tests of a major technology company's top-end server, crippling sales. The company spent more than $1 million trying to track down the cause of the failure. The perpetrator copied seven years worth of a colleague's e-mail records and transferred confidential corporate information outside the company, deleting records of his actions.[2]

**— U.S. Bank**

*Hacking and Cyber Extortion*

Organized hackers gained unauthorized access to computer systems, stealing the data of 56,000 credit cards and consumer financial information. They attempted to extort money from the bank, threatening to expose information publicly or damage the victims' computer systems. Damages were in excess of $700,000.[3]

### The stark reality is ...

U.S. companies suffer more than $13 billion in damages caused by security breaches. *[InformationWeek August 12, 2002]*

Courts have ruled that electronic data, software and other information assets that are housed in and communicated through computer networks are *in fact intangible, and therefore might NOT be covered under traditional insurance policies.*

**For more information, please contact your regional Lexington property representative.**

## Getting Started: Key Questions To Ask Your Client

1. **Does your company maintain sensitive or confidential data such as client information?**
   - Do you know the financial cost of restoring or recollecting that data if it were damaged in a computer attack?
2. **Is a functioning computer network important to the operations of your company?**
   - Would your business be adversely impacted if the network was shut down due to a computer attack? If so, do you know the financial cost in lost revenue and additional expenses associated with such an attack?
   - Would such a computer attack adversely impact your ability to service your clients? If so, do you know the financial costs associated with such a failure on your company?
3. **Has your company ever been hit with a mass computer virus such as NIMDA or Code Red?**
   - Do you know the total financial consequences of that event?
4. **Is your company vulnerable to a cyber extortion threat?**
   - Do you have a crisis management plan in place that includes specialized cyber extortion responders?
   - Do you know the total financial costs associated with responding (or not responding) to a cyber extortion threat?
5. **Have you fully evaluated the financial impact of a potential cyber terrorism attack?**

**Unless your client has fully accepted the financial costs associated with all of the above questions, your client should consider LexCyberSecure which provides coverage for certain exposures.**

## About Us

*Lexington Insurance Company, is one of the world's leading property and casualty companies whose products are marked by innovation, adaptability and flexibility and include a broad range of core business lines including: Property, Casualty Programs and Healthcare.*

*Underwriting services provided in conjunction with AIG eBusiness Risk Solutions (AIG eBRS). Lexington holds the highest financial strength ratings from our industry's principal rating agencies: A++ (Superior), Class XV, by A.M Best Company and AAA-rated by Standard & Poor's.*

[1] Daniel Tynan, "Dawn of the Superworm," *PC World Magazine* May 2003.

[2] Stephen Shankland, " Employee Sabotaged Superdome Tests," *CNET News.com* 8 November 2001.

[3] "Russian Computer Hacker Indicted in California for Breaking into Computer Systems and Extorting Victim Companies," *USDOJ.com* 20 June 2001