THE CIP REPORT

CRITICAL INFRASTRUCTURE PROTECTION PROGRAM VOLUME 6 NUMBER 3

SEPTEMBER 2007

CYBER INSURANCE

GEORGE MASON UNIVERSITY
School of Law
CRITICAL INFRASTRUCTURE PROTECTION PROGRAM

This issue of *The CIP Report* is focused on Cyber Insurance, a growing and complex industry confronted with the task of protecting companies against losses resulting from failures in computer networks. This umbrella term covers a wide range of protections, such as data theft, internal sabotage and theft, viruses, copyright infringement, and external hacking, to name a few. Adding to the complexity of providing this coverage is the difficulty of identifying and measuring cybersecurity risk, based on the lack of industry data and the ambiguous nature of cyber risk. Despite these challenges, the cyber insurance marketplace has grown to be a $350 millions business, with companies from every sector growing increasingly aware of their dependence on cyber networks and the necessity of secure critical technological infrastructures.

Building from a July 20th, 2007 event hosted by the CIP Program, the Workshop on Cybersecurity and Liability, this newsletter serves to collect background information on this complex topic, providing a state of the cyber insurance industry, insight from organizers from the event, an overview of the political landscape relating to cyber standards, highlights of landmark cyber cases, as well as perspectives from leaders within this industry.

We greatly appreciate the participation of Harry Oellrich and Sandy Hauserman of Guy Carpenter, both in this issue and the July event, as well as Robert A. Parisi, Tracey Vispoli, Toby Merrill, and J.T. Westermeier for lending their unique perspectives on this complex topic. We are also pleased to feature the work of two CIP Program law interns, Maggie Adkins and Joesph Maltby, both George Mason University Law students, in providing insight into the complex legal environment surrounding cyber liability. We hope you enjoy this issue of *The CIP Report* and thank you for your continued support of the CIP Program.

The State of the Cyber Insurance Industry

Less than a decade ago, the cyber insurance marketplace was virtually negligible, especially compared with more common life, health or property/casualty insurance. By late 2005, however, the cyber insurance marketplace had burgeoned into a $350 million business, pioneering a new kind of security – protection for companies against potential vast losses if their complex computer networks were to fail.

As businesses come to rely more on Internet technology, they are also becoming prone to high levels of risk in their day-to-day computer operations. Studies have shown that the world generated 161 billion gigabytes of digital information last year – equivalent to three million times the information in all books ever written, according to a 2007 white paper by ACE USA on cyber privacy. Not only could a computer network failure devastate a company's revenue stream, it could also invite expensive liability lawsuits if sensitive data, such as customer information, is lost or stolen. In the worst case scenario, a major cyber catastrophe could threaten to bring the entire nation's economy to its knees, given the interconnectedness of networks across the country.

Cyber Insurance is an umbrella term encompassing several kinds of insurance. It includes protection against:

- ✓ Data theft
- ✓ External hacking
- ✓ First- and third-party risks
- ✓ Internal sabotage and theft
- ✓ Computer malfunction
- ✓ Web content liability
- ✓ Viruses
- ✓ Copyright infringement
- ✓ Network outages
- ✓ Network congestion
- ✓ Copyright infringement and other areas related to technology

For additional background on the cyber insurance marketplace, see the June 2007 Betterley Report.

In the words Harrison Oellrich, Managing Director of Cyber Technology and Intellectual Property Practice, Guy Carpenter and Company, Inc., "Issues of homeland security are of critical importance, but concerns should not be exclusive to government agencies and entities. Like first responders, when bad things happen, people immediately look to the government or the insurance/reinsurance industry to maintain or preserve liquidity. The private sector has a critically important role to play in emergency preparedness and in ensuring that our national infrastructure is as secure as possible."

Industry Growth Stunted by Unknowns

As the concept of cyber risk becomes more tangible to firms, the role of cyber insurance grows more acute as part of the nation's plan to secure its critical technological infrastructure. Yet cyber insurers and reinsurers have progressed at a frustratingly slow pace, with major obstacles preventing development into a full-fledged industry.

Harrison D. Oellrich, a Managing Director of Guy Carpenter, has assumed a leadership role in several joint public/private initiatives designed to work collaboratively with the Federal Government to create a more secure internet/network environment. He has advised the White House, The Office of Homeland Security, Office of Cyberspace Security, Critical Infrastructure Assurance Office, and was a founding member and sector coordinator for the insurance/reinsurance sector's working group of the President's Critical Infrastructure Protection Board.

Much of the problem is rooted in a lack of industry data, as well as the ambiguous and volatile nature of cyber risk. Identifying and measuring cybersecurity risk is particularly daunting, for there are no established ways to truly capture the potential catastrophic consequences that could arise in the event of a disruption. As it stands, reinsurers do not have enough data to safely evaluate and support primary company policies. Even if brokers and underwriters are able to sell policies to customers, an insurance market

(Continued on Page 3)

Insurance Industry *(Cont. from 2)*

cannot develop without the support of the reinsurance community.

Another obstacle to industry growth is a lack of awareness among businesses about the liabilities they face in cybersecurity. For example, many firms do not know or understand cyber insurance as a product. Others fail to recognize the need for cyber insurance, even though purchase of many other kinds of insurance have become universally accepted concepts. In addition, courts also have passed conflicting judgments on where cyber-related liability resides. *[See legal cases, p. 9]* Finally, businesses lack basic corporate standards for cyber liability by which insurers and their reinsurers could better measure risk.

Because of these and other concerns associated with cyber insurance, insurers have been hesitant to cover cyber liabilities under existing property policies, stating that network systems do not qualify as "tangible property." Instead, many have opted to cover cyber risk through a limited array of additional insurance products, which of necessity have had to provide limited coverage at a relatively high cost.

Private Sector Pushes Partnership with Lawmakers, CIP Program

A solution to the many obstacles facing cyber insurance will involve a committed partnership between the government and private sector to create an environment in which the industry can develop and become economically viable.

Key private-sector firms have played a leadership role by persistently keeping the issue on the radars of security and insurance stakeholders. Guy Carpenter, a global risk and reinsurance specialist, has worked to highlight the potential for both market growth and improvement in the nation's economic security. Without a solid reinsurance industry, the cyber insurance industry as a whole will not be sustainable, given the significance of the reinsurance industry in accurately assessing and spreading risks.

Guy Carpenter also has spearheaded efforts to bring about more dialogue among the necessary stakeholders. Last July, lead by Harry Oellrich, Managing Director of Cyber Technology and Intellectual Property

(Continued on Page 11)

PARALLELS:
The Environmental Liability Insurance & Cyber–Risk

Sandy Hauserman
Senior Vice President
Environmental Specialty Group Practice Leader
Guy Carpenter & Co. Inc.

Sandy Hauserman has 26 years of experience in the insurance and reinsurance industry as a reinsurance intermediary and environmental attorney.

The 1980's witnessed the introduction of the absolute pollution exclusion into casualty policies due to court decisions construing the meaning of pollution liability. The need for environmental liability coverage remained, however, as environmental laws were increasingly being utilized to extract liability for pollution. Insurers then designed stand-alone environmental liability policies based on the requirements of environmental laws. Although coverage was initially narrow and expensive, as carriers became more comfortable with the coverage and confident in their underwriting protocols they expanded coverage. Now, 20 years later, these carriers are offering much broader coverage and at competitive rates.

Market development for environmental insurance managed to succeed because government statutes and regulation set environmental standards, making loss calculation possible and widening the risk pool to the point that insurance was profitable to offer. At the same time, regulatory standards and associated business reporting requirements provided data and information needed by the industry to model and appreciate risks and to develop appropriate environmental liability products.

In the field of property insurance, the idea that a building can and should be insured against a range of risks has become so commonplace that building codes now parallel the standards for insurability. Such is the potential with cyber liability.

Perspectives on Cyber Insurance

A Broker's Perspective:

Q&A With Robert Parisi

Q: The concept of cyber insurance is new to many firms, even though they rely so extensively on computers and information technology to operate their businesses. What are some of the new risks we face with the emergence of new technologies and information networks? Why is it so critical for brokers like Marsh to be engaged in developing this industry?

A: The Internet and information technologies have been incredibly dynamic in changing how businesses operate. Companies are able to store and share data across complex networks, and they can do it with greater efficiency than ever before – particularly in accessing data, marketing their products, and maintaining vendor relations. But while we enjoy the benefits of e-business strategies and Internet-based technologies, we are finding ourselves face-to-face with new risks and exposures that were unheard of just a decade ago. These include anything from data theft, external hacking, or the manipulation of sensitive information, such as customer financial or health records. Information networks also can be shut down by simple computer viruses that damage software and effectively disrupt business operations.

Robert A. Parisi, Jr is Senior Vice-President & National Technology, Network Risk & Telecommunications Practice Leader of the FINPRO unit of Marsh USA.

In addition, the regulatory environment has changed dramatically in the last few years. No longer is it just financial intuitions and healthcare companies that have to worry about how they handle data. The patchwork quilt of state privacy breach notification laws imposes a duty on all commercial entities that handle or collect personal information.

All of these factors present a whole new world of risks for the insurance industry. We, as experienced brokers, are continually exploring creative ways to insure customers against these new risks. Privacy and cyber insurance is a tough business because it is very much uncharted territory. We lack the full breadth of data necessary to create the kinds of risk models used for traditional insurance. To answer the second half of your question, it is extremely critical for brokers to be persistent about privacy and cyber insurance because not only are companies losing money over privacy breach and cyber-related failures, the nation's economy and security depend on it.

Q: Cyber insurance refers to day-to-day systems failures, but it also encompasses losses in the event of a catastrophic natural disaster or a terrorist attack. How does cyber terrorism require a new approach for brokers compared with our general understanding of insurance?

A: Cyber security disruptions can happen for a number of reasons, whether it is an accidental deletion of data or a deliberate attack from outside, or, more troubling, from an insider. With terrorist attacks, it complicates the matter even more because terrorism is so ambiguous by nature. The proportions of a cyber terrorist attack are difficult to predict – sometimes even to imagine. We have never experienced one before, at least not on the scale we are talking about. Also, cyber terrorism is inherently different from the traditional views of physical terrorist attacks. Whereas you can expect a physical terrorist attack to be somewhat localized, a cyber attack could potentially affect interconnected network systems across the nation, all at one time. The attack could spread to millions of people and essentially incapacitate them in a matter of minutes or hours. For all of these reasons, it is difficult for insurers to effectively price their products and to reserve capacity for their potential exposure to catastrophic terrorism losses.

[The] same policies and procedures that businesses take in protecting their computer systems from the ordinary hacker afford them protection from the cyber terrorist.

The flip side, however, is that the same policies and procedures that businesses take in protecting their computer systems from the ordinary hacker afford them protection from the cyber terrorist. So, it becomes a question of education and awareness *(Continued on Page 5)*

Perspectives *(Cont. from 4)*
about sound business practices. Cyber insurance calls for a unique approach, compared to the more traditional insurance with which we're familiar. At Marsh, our philosophy is always to engage in proactive risk consulting with our firms so we can anticipate new trends. By maintaining a dialogue with our customers, as well as industry stakeholders like government regulators, lawmakers, reinsurers and underwriters, we can pre-empt potential risks before they become costly problems. That way we won't have to learn about them in tomorrow's headlines.

Q: What are some of the ways brokers can or have provided greater protection against privacy and cyber risks for their customers?

A: Privacy and cyber risk is challenging because it is new not just to the customer, but for the broker and insurer as well. These days, you constantly have new technologies emerging that help firms run their business more efficiently, but also expose them to greater risk.

To deal with this, Marsh has been working with insurers across all lines to find the best ways to protect customers from all kinds of risks – everything from legal liability to copyright defamation to network outages to website defacement, among other things. We work with firms on all kinds of technology, like software, hardware and peripherals, data networking and infrastructure, Internet and new media, semiconductor and capital equipment, tech services and nanotechnology.

As a broker, Marsh uses risk analysis for new products, markets, operations and cyberspace exposure. We also use industry-specific benchmarking because we recognize that industries can have unique issues.

Underwriters' Perspectives:

Tracey Vispoli, Vice-President Chubb and Son

Q: Despite growing awareness about the need for cyber insurance, underwriters have trouble providing the coverage due to lack of data and other issues. Given these impediments, what is an underwriter's role in helping to nurture the industry?

A: There is little doubt that cyber risk is an important issue, not just for individual businesses but as a national security issue. Certainly there are a lot of obstacles to overcome before cyber insurance becomes a full-fledged industry, but we recognize how important it is to our firms. We also recognize that all stakeholders need to be involved in building the foundation for cyber insurance to become an economically viable industry. To help educate the insurance industry on the growing trend of cyber risks, Chubb has developed a series of continuing education courses for Insurance Agents and Brokers to help learn about the emerging cyber threat and gaps in traditional insurance policies. We also deliver risk management courses to customers on cyber exposures, network security best practices and disaster recovery.

Chubb has also developed a variety of insurance policies that help protect against different aspects of cyber risk. As an example, we recognize that our financial institution firms operate in a highly technology-dependent business environment. Our CyberSecurity insurance policy covers cyber risks for financial institutions and other commercial companies such as, manufacturing, retail, healthcare and professional services firms. The CyberSecurity policies help protect against losses caused by cyber attacks, employee breaches of network security, hackers, and the associated liability of these events. The policies also provide protection for consequential expenses such as, privacy breach notification expenses, crisis management expenses and reward expenses. We also have the ForeFront Portfolio Internet Liability Insurance, which protects businesses against liability over their website content.

On our company website we also provide free handbooks and papers that explain the growing importance of cyber insurance. Most people don't realize that property policies generally cover physical damage to "tangible property." They do not cover intangible property like data.
(Continued on Page 6)

Tracey Vispoli is a Vice President with property-casualty insurer Chubb & Son Inc., Warren, NJ. Ms. Vispoli is the worldwide manager of the Corporation's financial fidelity (crime) insurance business as a member of Chubb Specialty Insurance, a division of Chubb & Son. Ms. Vispoli is also the global Cyber Solutions Manager. "CyberSecurity by Chubb" is her latest marketing innovation.

Toby Merrill is an Assistant Vice President in ACE USA's Professional Risk division, where he is the national product manager of the Network Security, Privacy and Technology Liability products. In this capacity, he is responsible for product development as well as overseeing Network, Privacy and Technology E&O underwriting operations. Mr. Merrill has more than eight years' experience in the insurance arena, specifically in underwriting professional liability, management liability and cyber risk exposures.

Perspectives *(Cont. from 5)*

Toby Merrill, Assistant Vice-President, ACE Professional Risk

Q: The amount of exposure to network security risk is greater than ever, and yet the cyber insurance industry faces many obstacles to becoming fully economically viable. What makes it critical that this industry develop, and how does ACE see its role in the industry's development?

A: In the spring, ACE USA released a white paper that touched on this issue in depth. Privacy risk has always existed. However, in the past, it was inherently limited by physical constraints. At most, you might lose a briefcase or a file cabinet full of sensitive information. With the technology that we have today, you could easily lose a gigabyte of information in something as small as the USB thumb drive on your keychain. The amount of information stored there is equivalent to an entire pick-up truck full of printed social security numbers, credit card numbers or health records.

Another aspect of risk is the growing amount of regulation around consumer privacy. This includes, depending on a company's type of business, the Gramm-Leach-Bliley Act of 1999, the Health Insurance Portability and Accountability Act, the Federal Trade Commission Act, the Sarbanes Oxley Act and the more recent Payment Card Industry Data Security Standard, which took effect in 2006. All of these have set reasonable standards of care for internal controls and data security. But regulations enacted at the state level have had an even greater impact. In roughly three dozen states, companies are now required to notify consumers when their personal information has been exposed to potential fraud. According to data provided by the Privacy Rights Clearinghouse, prior to these notification laws the average frequency for a reported breach was once a month – today it is once a day. These state identity theft notification laws have now made it illegal to brush privacy breach events under the rug. This has forced companies to incur significant notification and public relations costs when their customers' information has been exposed, and in many cases, leads to defense and legal liability costs as well.

This is obviously a dangerous risk for any company holding sensitive customer information. Even the slightest hint that a company's information security was ever exposed or vulnerable could be a death knell for a company whose business depends on customer trust. That is why ACE is committed to creating an insurance policy that covers these risks. Many companies are wary of investing to improve their privacy controls, but our role is to highlight the true potential of these threats to damage a business and also to try to quantify the returns on their investments. ❖

Cyber Security Insurance Presents A Real Challenge

By J. T. Westermeier, Partner, DLA Piper

Cyber security insurance presents a real challenge to the insurance industry. Cyber security risks are increasing at an alarming exponential rate. They are increasing in frequency, volume, intensity, sophistication and severity. Legal standards with respect to these information security risks are just beginning to evolve and are far from certain. Designing an appropriate cyber security insurance policy for today's risks and tomorrow's cyber disasters is virtually impossible.

There is no actuarial database of legal actions arising from cyber security incidents. Identity theft is the country's fastest growing crime. Rapid advances in technology are constantly giving rise to new risks. This environment presents a formidable challenge to the insurance industry. Cyber security insurance products must reflect the needs of the customers and be priced prudently consistent with a realistic assessment of risks.

Cyber Standards: The Political Landscape

The number of incidents involving data security breaches is on the rise, leading policy makers to champion the need for national cyber standards for the private and public sectors.

In the last two years, more than 150 million individual records containing sensitive personal information have been compromised. This is cause for concern in light of the increasingly complex networks of sensitive information connecting the entire nation.

Lawmakers and policy leaders have responded in kind with various proposals for establishing cyber standards, which could help ensure that agencies and firms make basic, minimum efforts to safeguard sensitive information. Such standards would be critical for the viability of the Cyber Insurance industry, which currently suffers from a lack of benchmarks by which to accurately analyze risk.

Proposals for National Cyber Standards

The level of political interest in cyber standards is apparent in the number of current initiatives to develop them.

Administration

The need for cyber standards has been echoed by the President's Identity Theft Task Force, which recommended, in April of 2007, the development of a national data security protection standard for the private sector. The Task Force further recommended private sector entities be required by law to notify consumers and law enforcement in the event of a breach.

Independent Agencies

On the regulatory front, the Federal Trade Commission, which regulates false and deceptive practices, has stepped up enforcement activities in response to the threat of cyber security breaches.

The Federal Energy Regulatory Commission (FERC) also is in the process of approving eight Critical Infrastructure Protection Reliability Standards submitted by the North American Electric Reliability Corporation (NERC) in August of 2006. The standards encompass cyber security measures, and specifically require users of the Bulk-Power System to comply with certain standards to safeguard critical cyber assets.

Trade Groups

Even industry groups have taken the initiative to address cyber security, acknowledging that liability in privacy law is evolving not just domestically but internationally as well. Because of the global nature of the Internet and business, international compliance is a complex task involving different localities with differing privacy philosophies.

The American Institute of Certified Public Accountants (AICPA), which sets accounting standards for public companies, recently expanded its 10 privacy principles to incorporate domestic and international privacy laws. The new standards, called the Generally Accepted Privacy Principles (GAPP), set a high global standard for security measures and *(Continued on Page 8)*

'9/11 Law' Expands Preparedness Expectations to Private Sector

Following passage of the new '9/11 Law' last month, the private sector could face homeland security preparedness expectations for the first time ever, based on new voluntary standards.

Officially called "Implementing Recommendations of the 9/11 Commission Act of 2007," the law directs the Department of Homeland Security (DHS) to establish a voluntary accreditation and certification program to assess the preparedness of private sector entities to respond in emergency situations. A designated officer will develop "voluntary preparedness standards" – a common set of criteria for preparedness, disaster management, emergency management and business continuity programs – by which private sector entities can be certified if they voluntarily seek certification.

In accordance with Sec. 902, the DHS Private Sector Office will provide information to the private sector regarding these standards and the business justification for adopting them.

Standards *(Cont. from 7)*
are available for government agencies and corporations of all sizes to use to improve management of sensitive data.

Lawmakers

Finally, Congress has been abuzz with proposed legislation to address privacy and data security (*see sidebar*). Even beyond the Federal level, the number of states requiring disclosure of security breaches is growing – at least 36 states now have data breach notification laws for the private sector.

Trends & Stumbling Blocks

The recent attention toward cyber standards reflects three key national trends:

1) The responsibility of all entities holding sensitive personal information to provide security is expanding;
2) The legal standard for what is considered reasonable security is evolving; and
3) Data security frameworks must be risk-based and reflect a comprehensive approach to information security management.

Despite the political interest in establishing national cyberstandards, however, there remains intense debate over how exactly these trends should continue unfolding.

One question explores the fine balance between federal and state jurisdiction. To what extent does federal authority pre-empt state law when it comes to cyber standards? Some consumer groups prefer a softer pre-emption that preserves the authority of state bills that impose stronger standards. Regulated industry sectors often prefer enforcement authority be limited to the appropriate federal functional regulators.

The question of enforcement authority also poses similar questions. Some state Attorneys General seek to maintain enforcement authority in the area of cyber standards. Consumer groups also demand preservation of a private right of action in the event of any new law.

Congress has faced impediments that reflect the new nature of the cyber standards issue. Within both houses of the 109th Congress, six different committees asserted jurisdiction over cyber security, impeding progress on bills that might have established standards for protecting sensitive personal information held by private sector entities. Agreement on these issues needs to be reached in order for the bills to be enacted. ❖

Congress Aims to Establish Cyber Standards

The following bills have been introduced in the 110th Congress. All would establish security standards to reduce the likelihood of a breach and require notification in the event that a breach does occur.

- ❑ The Personal Data Privacy and Security Act of 2007 (S.495): Introduced by Sen. Patrick Leahy (D-VT) and Sen. Arlen Specter (R-PA), chairman and ranking member of the Senate Judiciary Committee. This bill was marked up by the Judiciary Committee on May 3.
- ❑ The Data Accountability and Trust Act (HR.958): Introduced by Rep. Bobby Rush (D-IL) and Rep. Cliff Stearns (R-FL), this is the House Energy and Commerce bill. There has been no committee action as of yet.
- ❑ The Identity Theft Prevention Act (S.1178): Introduced by Sen. Daniel Inouye (D-HI) and Sen. Ted Stevens (R-AK), chairman and ranking member of the Senate Commerce Committee. This bill was marked up by the Commerce Committee on April 25.
- ❑ The Data Security Act of 2007 (S.1260): Introduced by Sen. Tom Carper (D-DE) and Sen. Robert Bennett (R-UT), considered a key Senate Banking bill. It is also possible that Senate Banking Chairman Chris Dodd (D-CT) may decide to introduce his own bill. There has been no committee action as of yet.
- ❑ Draft Financial Services Bill: A new House Financial Services bill is currently being drafted. Chairman Barney Frank (D-MA) and Rep. Melissa Bean (D-IL) will take the lead on this bill.

Liability Landmarks: Important Cyber Cases Forming the Legal Environment

Maggie Adkins and Joseph Maltby
CIP Program, Law Interns

During the Cyber Liability workshop, participants from the insurance and reinsurance industry cited several precedent-setting federal cases that constitute the current legal landscape on cyber liability. We examined and summarized these cases to provide readers of this *CIP Report* with a legal framework, starting with the most recent, *Choicepoint*, in which the defendant was fined $10 million by the Federal Trade Commission (FTC).

United States of America v. Choicepoint Inc.

UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF GEORGIA

(http://www.ftc.gov/os/caselist/choicepoint/choicepoint.shtm)

February 10, 2006

Choicepoint, a data management company, settled a controversy with the FTC out of court involving Choicepoint's loss of a large amount of customer data. While, as a settlement, this case does not hold any value as precedent, it can influence future settlements and even decisions. Choicepoint agreed to a $10 million fine and also limited its business activities. This included a ban on the furnishing of consumer credit reports to unauthorized third parties. Choicepoint also agreed to create a system of protections to avoid future incidents. These protections included procedures to review third party applications for consumer credit reports as well as a reasonable system of information security protections for customer data. As the stipulation stated, "at a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (a) employee training and management; (b) information systems, including network and software design, information processing, storage, transmission, and disposal; and (c) prevention, detection, and response to attacks, intrusions, or other systems failures." This program must also include testing procedures, in an effort to prevent similar mishaps in the future.

American Online, Inc. v. St. Paul Mercury Insurance Company

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT

347 F.3d 89; 2003 U.S. App. LEXIS 20928

October 15, 2003, Decided

This is an appeal by AOL after a judgment in favor of St. Paul Mercury Insurance Company (St. Paul). After AOL released a new version of Access software, consumer class action suits were filed alleging that Access software altered their software, disrupted their network connections, caused the loss of stored data and caused their operating systems to crash. St. Paul denied the claim, stating the damages claimed by the consumers were not "property damage to tangible property" as defined by the policy. The district court granted summary judgment to St. Paul on the grounds that the consumers' underlying complaints did not allege physical damage to tangible property and that any damage from loss of use of the computers as tangible property fell within the impaired property exclusion. The court affirmed the judgment in favor of St. Paul, concluding that the complaints involved software problems and that software and lost data are not "tangible property," so coverage for consumers' loss of use of their computers was barred.

American Guarantee & Liability Insurance Company v. Ingram Micro, Inc.

UNITED STATES DISTRICT COURT FOR THE DISTRICT OF ARIZONA

2000 U.S. Dist. LEXIS 7299

April 18, 2000, Decided

(Continued on Page 10)

Cases *(Cont. from 9)*

Ingram Micro, Inc. (Ingram), a computer products distributor, obtained an insurance policy from American Guarantee Liability Insurance Company (American) against all risks of direct physical loss or damage to property and business income. Ingram subsequently suffered a power outage that disrupted operations; as a result some computers had to be manually reprogrammed due to memory loss. However, their claim for the loss was denied by American. American then filed an action for declaratory relief stating that Ingram's loss was not covered by the insurance policy. Ingram filed a counterclaim for breach of contract. Both parties filed motions for partial summary judgment. The court granted Ingram's motion and denied American's motion, holding that Ingram's computers were physically damaged under the terms of the policy. The court found that physical damage under the policy was not limited to physical harm to defendant's computers, but included the loss of the computers' use or functionality. Because Ingram's computers' data was unavailable, services were interrupted, and the programs were altered, Ingram suffered physical damage. This case was distinguished from Seagate because Ingram alleged property damage that had to be repaired, while in Seagate the damage caused by the defective product did not damage the entire computer.

Seagate Technology, Inc. v. St. Paul Fire and Marine Insurance Company and Cigna Property and Casualty Insurance Company

UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF CALIFORNIA

11 F. Supp. 2d 1150; 1998 U.S. Dist. LEXIS 13322; 98 Daily Journal DAR 11477

May 15, 1998, Decided

Seagate manufactures disk drive storage devices for personal computers and small business machines. Amstrad, a UK corporation, purchased Seagate disk drives for its personal computers it began selling in 1989. In 1991 Amstrad sued Seagate, claiming that the drives were defective. Judgment favored Amstrad. That year Seagate tendered its insurance coverage claim based on the Amstrad action to St. Paul and CIGNA insurance companies. St. Paul and CIGNA both denied Seagate's claim and on June 7, 1994, Seagate brought suit against St. Paul and CIGNA. Seagate's complaint brought causes of action for breach of contract and tortious bad faith based in part on St. Paul's refusal to defend Seagate in the Amstrad actions. On February 20, 1998, Seagate and the insurance companies each sought summary judgment in their own favor. The court found for the insurance companies, noting that the language of the insurance policies indicated that the duty to defend only arose if the damage or injury alleged by the party suing the insured could be read to constitute physical damage to the tangible property of others. The court agreed with St. Paul that incorporation of a defect into the property of another could not constitute the physical damage to tangible property needed to warrant coverage under the policies. The court found that the Armstrong rule was inapplicable to the case, which involved allegations of defective design or manufacture of a product, rather than an inherently dangerous product. The court concluded that as there were no allegations of physical harm to the whole, the underlying lawsuits failed to allege "property damage" within the meaning of the umbrella policies and St. Paul thus lacked a duty to defend those actions. ❖

Insurance Industry *(Cont. from 3)*
Practice, the firm helped to facilitate the Critical Infrastructure Protection (CIP) Program Workshop on Cybersecurity & Liability – a multi-stakeholder dialogue on how to address impediments to cyber insurance. Representatives from American Insurance Group, the Chubb Group, ACE INA, as well as Congressional staff and George Mason University Law School professors discussed in-depth reasons for why the cyber insurance industry has not taken flight. They also addressed creative ways to use existing models to overcome the lack of data available for the cyber insurance market.

MAIN OBSTACLES TO CYBER INSURANCE

Lack of Data: Reinsurers do not have adequate data to accurately model and therefore price their policies.

Awareness: In most companies, risk managers and business continuity executives who make insurance-purchasing decisions are not aware of data loss risks and cyber liability issues. On the other hand, IT experts assume they have taken all the necessary security measures, such as firewalls and antivirus programs, and do not like to admit that there are still significant risks to their networks.

Accountability: Standards for corporate accountability for cyber liability are unclear. Therefore, nobody shoulders responsibility for the risks, which remain unaddressed.

Standards and Best Practices: Basic industry-wide standards are virtually nonexistent when it comes to cyber security. This lack of standardization makes it difficult for insurers and reinsurers to accurately analyze risk and price insurance policies.

Participants pointed out that although the nature of insuring against cyber attack is fundamentally different from insuring against physical or health damages, there are lessons to be learned from the successes of physical insurance. For instance, insurers and reinsurers were successful in developing a robust property insurance industry because the government established safety codes and product standards to regulate buildings and physical assets. Insurers were able to measure risk reduction based on data already required by contractual and regulatory structures. Similarly, government regulators and lawmakers could play a key role in establishing the foundation for data collection and risk measurement. *[See cyber standards, p. 7]* Debate continues, however, over whether government intervention in the cyber sphere is desirable or if insurers should simply impose basic cyberstandards when governmental regulation is not forthcoming. ❖

"[We need a] comprehensive loss prevention and business recovery protocol – a roadmap if you will – for managing risks enterprise-wide that critical infrastructure industries can follow."
Dean O'Hare, Chairman, Chubb Group

The CIP Program works in conjunction with James Madison University and seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems and economic processes supporting the nation's critical infrastructure. The CIP Program is funded by a grant from The National Institute of Standards and Technology (NIST).

The CIP Report is published by Zeichner Risk Analytics, LLC (ZRA) on behalf of the CIP Program. ZRA is the leading provider of risk and security governance knowledge for senior business and government professionals. ZRA's vision is to be a consistent and reliable source of strategic and operational intelligence to support core business processes, functions, and assurance goals.

If you would like to be added to the distribution list for The CIP Report, please click on this link: http://listserv.gmu.edu/cgi-bin/wa?SUBED1=cipp-report-l&A=1