SEIGER GFELLER LAURIE LLP
ATTORNEYS AT LAW

Presentation to Holborn on Cyber Risks and Insurance

November 3, 2016

Agenda

- Overview of cyber risks
- Potential coverage under Property and CGL policies
- Potential coverage under Crime and Computer Fraud policies
- Potential coverage under Cyber policies

Principal Cyber Risks

- Data breaches of personal and confidential information
- Claims for failure to maintain adequate cybersecurity
- Network disruption / business interruption
- Lost or degraded data
- Fraudulent funds transfers, through hacks, social engineering, employee negligence, or some combination
- Cyber extortion and ransomware
- Liability arising from websites, social media, and other media liability risks
- Liability for technology risks in providing computer services or products

Exposure of Insurance Companies

Insurance companies are exposed to all of these, especially data breaches and corresponding claims for failure to maintain adequate security. They and their directors are subject to potential liability when data breaches and cybersecurity failures occur.

Insurance companies must take into consideration various sources of regulatory requirements and guidance. Some are in effect, and others are pending.

NAIC

- In March of 2016, the Cybersecurity Task Force released a preliminary working Draft of an Insurance Data Security Model Law. On August 17, a revised draft was released. The Model law expressly requires oversight of cybersecurity by the Board of Directors. The NAIC has been moving at breathtaking speed by insurance standards. It says it will try to have the Model Law complete and approved by the end of this year.

The New York Department of Financial Services

- On September 13, the DFS announced a proposed regulation, Cybersecurity Requirements for Financial Services Companies.

State Pre-Breach Security Measure Laws Not Specific to Insurers

- Many states have laws requiring pre-beach security measures, generally requiring that they be "reasonable."

- The California Attorney General February 2016 Data Breach Report states that failure to implement the Center for Internet Security's Critical Security Controls constitutes a lack of reasonable security.

Other Sources

- Department of Homeland Security National Infrastructure Protection Plan Financial Services Sector-Specific Plan

- National Institute of Standards and Technology ("NIST") Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity

- Federal Trade Commission

- SEC

- International Association of Insurance Supervisors

- EU-US Privacy Shield

Exposure of Insured SMEs

Small- and medium-sized enterprises are the prime targets for cyber attackers because they tend to be easier targets. Precise numbers do not exist, but many sources estimate that the majority of cyber "attacks" (mostly cyber crimes) are directed toward SMEs.

- Nationwide (the largest insurer of small businesses) conducted a survey in 2015 that indicated 63% of small businesses have victims of at least one kind of cyber attack.

- The Ponemon Institute reported that 55% of SMEs had experienced a cyber attack from June 2015 through July 2016.

- A recent National Cyber Security Alliance study indicates that more than 70% of cyber attacks are directed at small business, and almost 50% of small businesses have actually *experienced* an attack, and that as much as 60% of those that experience a data breach go out of business after six months.

- Fireye estimates that 77% of cyber crimes so far in 2016 targeted SMEs.

Key Trends

Ransomware. The most noteworthy trend is the rapidly increasing pace of ransomware attacks. These attacks deny a company access to its computer network, often by encrypting the data, and demanding payment of a ransom, typically in Bitcoin, the restore access. Financial services and health care are most commonly targeted, but even small retailers are targets. The criminals have found an effective pricing strategy. The demand is usually between $300 and $500 (with others at $10,000-20,000 or higher), yet the frequency is so great that annual losses are at least tens of millions of dollars. The technology is not especially difficult to master, and "ransomware as a service" is available. Some syndicates will "license" their exploit kits to others, in exchange for a share of any profits made. Beyond the ransom payment itself, there are often business interruption losses and forensic and repair expenses. SMEs often take weeks or months to recover.

- The FBI says that in 2016, more than 4,000 cases of ransomware have occurred each day. This is four times the rate from last year.

- Beazley released a report saying that as of October 2016, its clients have been the target of 150 ransomware attacks, with 52 coming in July and August. It estimates that, consistent with the FBI report, it will see four times as many ransomware attacks this year as last.

Fraudulent Funds Transfers. Whether accomplished by outside hackers acting independently, or the result of social engineering, sometimes compounded be employee negligence. There are substantial coverage issues under existing policies, and a neew market is developing. This will be discussed below.

Potential Coverage Under Property Policies

- There is a possibility that coverage will exist for certain losses, notably network disruption, business interruption, and lost data, unless they are subject to an exclusion. Several cases from 2000 to 2006 found such coverage.

    - ***Am. Guaranty & Liability Ins. Co. v. Ingram Micro, Inc.,*** 2000 WL 726789 (D. Ariz. Apr. 18, 2000) (found coverage for network disruption caused by a power surge under an all risk policy insuring against "direct physical loss or damage from any cause, howsoever and wheresoever occurring").

    - ***NMS Services, Inc. v. Hartford***, 62 Fed.Appx 511 (4th Cir. 2003) (found coverage under a computer endorsement to a property policy for erasure of computer files and databases by a disgruntled former employee).

    - ***Lambrecht & Associates, Inc. v. State Farm Lloyds,*** 119 S.W.3d 16 (Ct.App.Texas 2003) (found coverage under the property portion of a business policy for a hacker attack resulting in network disruption, lost data, business interruption, and the cost of replacing a server and software packages).

    - ***Southern Mental Health Center, Inc. v. Pacific Ins. Co. Ltd***., 439 F.Supp2d 831 (W.D.Tenn. 2006) (found coverage for business interruption under an all risks policy after a storm and power outage caused data loss to a pharmacy's computer, because corruption of data constitutes "direct physical loss or damage to property").

- One case reached a contrary result.

    - ***Ward General. Ins. Servs., Inc v. Employers Fire Ins. Co.,*** 7 Cal. Rptr.3d 844 (Ca.App.Ct. 2003) (found no coverage under a property policy for a system crash and loss of data, because data is merely "information" without a "material existence," so could not suffer "direct physical loss").

- To counter these cases, many property policies have historically contained cyber exclusions.

- However, over the course of the last year or so, the soft property insurance market is leading many insurers to offer coverage for cyber-related risks, not only

for “physical loss” but also for loss of digital assets and business interruption caused by cloud failures.

- FM Global takes a prominent public position that its property policies cover cyber-related losses.
- Other insurers have accepted such losses without objection, in the absence of an exclusion.
- Property underwriters are seeing an advantage in affirmatively granting coverage for cyber-related risks, and are doing so.

Potential Coverage for Data Breaches Under CGL Policies

- Policyholders have sought to obtain CGL coverage following a cyber incident.
- Courts have split on these issues.
- Both Coverage A (Property Damage) and Coverage B (Personal and Advertising Liability) are being tested in litigation.

General Liability – Coverage A

- Most CGL policies afford coverage for “those sums that the insured becomes legally obligated to pay as damages because of … ‘property damage’ to which this insurance applies.”
- “Property damage” is defined to mean “physical injury to tangible property, including all resulting loss of use of that property” and “loss of use of tangible property that is not physically injured.”
- Under CGL policies issued before 2001, a split of authority existed as to whether electronic data constituted “tangible property.”
- ***Am. Online, Inc. v. St. Paul Mercury Ins. Co.,*** 207 F. Supp. 2d 459, 466 (E.D. Va. 2002) (“Computer data is not tangible property”), aff’d, 347 F.3d 89 (4th Cir. 2003).
- ***State Auto Prop. & Cas. Ins. Co. v. Midwest Computers & More****,* 147 F. Supp. 2d 1113, 1116 (W.D. Okla. 2001) (“Alone, computer data cannot be touched, held or sensed by the human mind; it has no physical substance. It is not tangible property.”).
- ***Computer Corner, Inc. v. Fireman’s Fund Ins. Co.*****,** 46 P.2d 1264 (N.M. Ct. App. 2002) (finding coverage for suit for loss of data from reformatting hard drive; “computer data is tangible property”).

- ***Am. Guar. & Liab. Ins. Co. v. Ingram Micro, Inc***., 2000 WL 726789 (D. Ariz. Apr. 18, 2000) (concluding that loss of data on computer network constituted "property damage").

- Some CGL policies specifically provide that "electronic data is not tangible property." See ISO Form No. CG 00 01 10 01 (added in 2001).

- More recent CGL policies eliminate coverage for "[d]amages arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data." See ISO Form No. CG 00 01 12 04 (added in 2004).

- Assuming this exclusion is applied as written, Coverage A should not afford coverage under post-2004 policies with this exclusion regardless of how the definition of "property damage" is construed.

General Liability – Coverage B

- Policyholders have also sought coverage for data breaches under "Coverage B," which covers "those sums that the insured becomes legally obligated to pay as damages because of 'personal and advertising injury.'"

- "Personal and advertising injury" is defined to include "injury … arising out of one or more of the following offenses: … [o]ral or written publication, in any manner, of material that violates a person's right of privacy."

- Policyholders are testing whether at least some types of claims arising from a data breach (*e.g.,* alleged failure to secure private data adequately) can fall under the "personal or advertising injury" coverage found in CGL policies.

- There are many coverage issues posed by these cases, and the early court rulings are mixed.

- ISO issued a set of exclusions to be included in CGL policies in May 2014 that bar coverage for claims "arising out of any access to or disclosure of any person's or organization's confidential or personal information."

- However, these exclusions may take some time to make their way into CGL policies and – even after they have been utilized – and policyholders likely will seek to litigate their scope of this exclusion in specific instances.

- The early cases addressing data breach, privacy and other cyber claims under CGL coverage are mixed.

- To the extent coverage is found, it has been limited to certain fact settings and to certain types of exposures. CGL coverage plainly does not encompass all data breach, privacy and cyber losses – even when courts find some coverage.

- ***Hartford Cas. Ins. Co. v. Corcino & Assocs.,*** 2013 WL 5687527 (C.D. Cal. Oct. 7, 2013).

    - Insured allegedly posted "private, confidential, and sensitive medical and/or psychiatric information" on a public website, which remained online for almost a full year. Patients brought class actions which sought, among other relief, statutory damages of $1,000 per person under the California Confidentiality of Medical Information Act ("CMIA") and statutory damages of up to $10,000 per person under the California Lanterman Petris Short ("LPS") Act.

    - Insurers contended coverage was barred under an exclusion for "Personal And Advertising Injury ... [a]rising out of the violation of a person's right to privacy created by any state or federal act." However, the court found that "the plaintiffs in the underlying cases seek remedies for breaches of privacy rights that were not themselves 'created by any state or federal act,'" but which exist under common law and the California state Constitution.

    - The court also rejected Hartford's argument that the statutory penalties were not covered "damages" because of "personal and advertising injury," finding that "[t]he statutes … permit an injured individual to recover damages for breach of an established privacy right, and as such, fall squarely within the Policy's coverage."

- ***Travelers Indem. Co. v. Portal Healthcare Solutions LLC****,* 14-1944 (4th Cir. Apr. 11, 2016) (unpublished).

    - Insured allegedly failed to safeguard confidential medical records from being viewed on a public website, and two patients (who later sued) alleged that they were able to access their own records by way of a Google search.

    - Trial court found a duty to defend based on potential coverage for "unreasonable publicity" to and "disclosure" of information about patients' private lives. It found "publication" to arguably include records "place[d] before the public," and a potential for coverage based on the underlying allegations, even though the insured took no steps designed to disclose or publish the information and there was no evidence it was viewed by any third party.

    - The Fourth Circuit affirmed the trial court's determination that the complaint at least potentially or arguably alleged conduct covered under the Policies.

- ***Zurich Am. Ins. Co. v. Sony Corp. of Am.,*** No. 651982/2011 (N.Y. Sup. Ct. Feb. 21, 2014).

    - Sony's PlayStation Network was hacked in April 2011. The hackers stole personally-identifiable information of over 77 million users, one of the largest data breaches in history.

    - Sony argued that hackers' theft of personal information fell within the Coverage B offense of "oral or written publication in any manner of material that violates a person's right of privacy."

    - The court ruled that coverage was not triggered where the alleged "publication" was not an intentional act committed by the insured, but instead was the result of a criminal act of a third party hacker. It held that the "oral or written publication" offense requires "an act by or some kind of act or conduct by the policyholder in order for coverage to be present."

    - The case settled while on appeal to New York intermediate appellate court.

- ***Recall Total Info. Mgmt., Inc. v. Federal Ins. Co.,*** 115 A.3d 458 (Conn. 2015)

    - Insured transport vendor allegedly lost data tapes containing sensitive data on a large number of employees of IBM. Those tapes allegedly were recovered by a third party, but there was no evidence that the information on the tapes was ever accessed. The main "damages" sought were the costs of notification and remedial measures allegedly taken by the party who owned the data tapes.

    - Court ruled that there was no "publication" absent evidence that information on the tapes was ever accessed, noting that the communication of information to a third party was required to trigger coverage.

    - The court also held that triggering a breach notification statute does not demonstrate personal injury as such statutes "merely require notification to an affected person so that he may protect himself from potential harm."

Coverage for Fraudulent Funds Transfers and Social Engineering

- Businesses face an endless stream of attempted fraudulent funds transfers. Losses from these schemes have not been covered by most cyber insurance policies, yet insureds instinctively think of them as "cyber losses."

- There are at least seven different potential scenarios for fraudulent funds transfers:

    1) The transfer can be effected entirely by a hacker remotely penetrating a computer system, and making the transfer;
    2) The hack and transfer can be enabled by employee negligence;
    3) The fraudster convinces an employee to reveal his credentials, and then enters the network by using them, to transfer funds;
    4) The fraudster gets an employee to open up an attachment, thereby allowing the network to be penetrated, and allowing the transfer of funds;
    5) The fraudster, through emails or telephone calls or both, posing as a company's executives, vendors or customers, convinces an employee to transfer funds;
    6) An employee enters data believed to be accurate, but which in fact is fraudulent; and
    7) A rogue employee makes an improper transfer or enters fraudulent data.

- Items 3, 4 and 5 are variants of methods which have come to be known as "social engineering," *i.e.,* the manipulation of humans into performing acts or divulging confidential information.

- Commercial Crime policies are often broadened to cover some forms of fraudulent funds transfers, typically by insuring agreements or endorsements for Computer Fraud and Funds Transfer Fraud.

- The application of Computer Fraud and Funds Transfer Fraud to fraudulent funds transfers involving computers, social engineering, and employee negligence has arisen in several recent cases. The main issues have been whether the policy applies to entries by authorized users or only to outside hackers, and whether there is causation when the deception involves multiple causes, such as emails, telephone calls, and employee negligence. Most of the decisions have held that there is no coverage. One U.S. Circuit Court, however, found coverage when an outside hacker's ability to transfer funds was enabled by employee negligence.

Decisions

- ***Universal Am. Corp v. Nat'l Union Fire Ins. Co. of Pittsburgh, PA****,* 25 N.Y. 3d 675 (2015).

    - Found no coverage under a financial institutions bond for losses arising when healthcare providers who were allowed to submit claims directly into the computer system of a health insurer (the insured) submitted over $18 million in fraudulent claims. The bond excluded "losses resulting directly or indirectly from fraudulent instruments which are used as source documentation in the preparation of Electronic Data, or manually keyed into a data terminal."

- Rationale: The Bond provided coverage for losses incurred through unauthorized access to the computer system, *i.e.,* deceitful and dishonest acts of outside hackers, but not to fraudulent information entered by authorized users.

- ***Pestmaster Services Inc. v. Travelers Cas. and Surety Co. of America,*** No. 14-56294 (9th Cir. July 29, 2016).

  - Affirmed a district court in holding that there was no coverage for lost funds transferred by the insured to a payroll company, which failed to remit the portion representing payroll taxes to the IRS.

  - Rationale: Neither the Computer Fraud nor the Funds Transfer Fraud insuring agreements applies where the transfer is made by an employee who was an authorized user of the system. Also, "[B]ecause computers are used in almost every business transaction, reading [the Computer Fraud] provision to cover all transfers that involve both a computer and fraud at some point in the transaction would convert this Crime Policy into a 'General Fraud' Policy."

- ***Apache Corp. v. Great American Ins. Co.*,** No. 15-204992015 (5th Cir. Oct. 18, 2016).

  - The court found no coverage for a social engineering induced transfer of funds under a Crime Protection Policy with a Computer Fraud provision, which insured against "loss . . . resulting directly from the use of any computer to fraudulently cause a transfer of [money] from inside the premises." The fraudster made a telephone call to an oil-production company, claiming to be an actual vendor, requesting that future payments be sent to a new bank account. Upon being told the request had to be in made in writing, the fraudster sent an email from an email address that was similar to the vendor's, attaching a letter purportedly on the vendor's letterhead, providing both the old bank account transfer number and the new one. An Apache employee called the telephone number on the letter, and concluded the requested change was legitimate. A different Apache employee approved and implemented the change, and in response to invoices from the actual vendor, transferred millions of dollars to the fraudster's account.

  - Rationale: the email was part of a scheme, but it was merely incidental to the occurrence of the authorized transfer of funds. If Apache had conducted a more thorough investigation, such as calling the correct telephone number known from past communications, it would never have changed the account information.

- ***Aqua Star (USA) Corp. v. Travelers Cas. and Surety Co. of America,*** No. C14-1358RSL (W.D. Wa, July 8, 2016).

    - This court also found no coverage under a similar scenario, this time involving a hack of a vendor of shrimp. The hacker directed the vendor's customer, a seafood importer, to change the bank account to which it made wire transfer payments. An employee of the importer did this and the company lost $713,890.

    - Rationale: The court applied an exclusion providing that the Policy "will not apply to loss resulting directly or indirectly from the input of Electronic Data by a natural person having the authority to enter the Insured's Computer System." It found that the actions of an authorized employee in effecting the wire transfers were an indirect cause of the loss, so coverage was barred. The case is on appeal to the Ninth Circuit.

- ***The State Bank of Bellingham v. BancInsure, Inc.,*** No 133432 2016 WL 2943161 (8th Cir. May 20, 2016).

    - Found coverage under a financial institution bond when a hacker broke into a network and performed fraudulent wire transfers, notwithstanding that the hack was enabled by employee negligence (leaving access tokens in the network overnight)

    - Rationale: The court applied the concurrent causation doctrine, and held that the "efficient and proximate cause" of the loss was the transfer by the hacker, not the negligence of the employees.

Industry Reaction

- Some insurers now offer Crime Policies that provide coverage for fraudulent funds transfers, either through direct hacks or social engineering. They tend to be subject to sub-limits, frequently $250,000.

- Also, an increasing number of ***cyber*** insurers now expressly provide coverage for these risks. According to The Betterley Report's June 2016 Cyber/Privacy Insurance Market Survey, of 31 cyber insurers surveyed, 13 offer some coverage for fraudulent funds transfers. Coverage is most often afforded with sub-limits of $250,000, although some insurers have sub-limits of $500,000 or $1,000,000, and possibly more, "subject to underwriting."
  .

Specific Cyber Coverage

- In 2015, the NAIC's Property and Casualty Insurance Committee created an Annual Statement Supplement called the Cybersecurity and Identity Theft Coverage Supplement. It requires all companies that provide cyber insurance, either as an add-on to commercial multi-peril packages or as a standalone product, to report the range of limits, losses paid, earned premium, whether policies were claims made, and whether tail coverage is offered. On June 30, 2016, it announced the first analysis of the 2015 filings. It found that more than 500 insurers have provided businesses and individuals with cyber insurance, the vast majority of which were written as endorsements to commercial and personal policies.

- Cyber or Data Breach endorsements to traditional package/CGL policies generally provide limited coverage and low sub-limits.

- ISO has a series of optional cyber coverage endorsements designed to be added to its Business Owners Policy. These are directed to SMEs. They offer three tiers of potential coverage, starting with breach response protection as the required coverage part.

    - The first tier provides First Party Coverages for security breach expense, public relations expense, and replacement or restoration of electronic data.

    - The second tier provides security breach liability coverage.

    - The third tier provides coverage for extortion threats, business income and extra expense, and web publishing liability.

    - There are also additional optional endorsements providing coverage for: PCI defense expenses; fines and penalties; and acts of rogue employees.

Standalone Cyber Insurance Policies

- Beyond these endorsements, there is an emerging and growing market of between 50 and 70 insurers writing standalone cyber policies. There are virtually no standard terms. Each company has its own manuscript form. Leading brokers have their own forms. Policy terms are negotiated.

- Most of these companies offer a suite of potential coverages that can include several "core" coverages.

First Party Loss, including:

- Data Breach Response / Security Event Costs
- Attorney / ”Breach Coach” fees, forensic review fees, notification costs, credit monitoring
- Public relations, etc.

.

- Network Disruption
- Business Interruption / Contingent Business Interruption
- Data Loss / Data Restoration
- Cyber Extortion and Ransomware

Third Party Liability, including:

- Privacy claims by aggrieved consumers, often brought in class actions
- Privacy Regulatory and PCI Liability
- Claims for inadvertent transmission of malware
- In some instances, downstream contingent business interruption

Media Liability, typically including:

- Invasion of privacy
- Infringement of the right of publicity
- Defamation, including libel and slander, product disparagement and trade libel
- Infringement of intellectual property rights
- Piracy, plagiarism and misappropriation of ideas
- Claims based on user-generated content

In this competitive market, some companies offer expansive optional Media Liability Coverages:

- Acts of rogue employees (which may be covered anyway, it the policy covers vicarious liability)
- Acts of independent contractors (and *their* rogue employees)
- Offline media, as well as online media
- International coverage
- False advertising
- Software copyright infringement claims
- Costs of defending and complying with injunctive relief
- Defense costs to object to subpoenas for production of information
- Unfair competition or unfair trade practices alleged in connection with other insured offenses, and
- Economic harm to third parties relying on false or erroneous content

Technology Errors and Omissions Liability

- Addresses exposures arising from an entity's technology services (consulting, customer software development, etc.) and products (software and hardware).
- Coverage is triggered by claims or suits arising out of an actual or alleged negligent act, error or omission.
- Coverage can also be triggered by claims arising from breach of contract.

vvitkowsky@sgllawgroup.com

rlaurie@sgllawgroup.com

Vince Vitkowsky *is a partner at Seiger Gfeller Laurie LLP, resident in New York. He represents insurers and reinsurers in litigation, counselling and product development in many lines of business, including cyber, E&O, D&O and CGL insurance. Vince represents cyber insurers on coverage issues, and reviews and drafts cyber policy language, and monitors the rapidly evolving cyber threat matrix. He created a Cybersecurity Podcast and Symposium Series featuring leading cyber experts, consultants, present and former government officials, and journalists. He is a former Adjunct Fellow at the Center for Law and Counterterrorism.*

Bob Laurie *is one of the founding partners in Seiger Gfeller Laurie LLP. He is a litigator with a broad-based practice, which includes representing insurers in disputes concerning coverage determinations, bad faith and extra-contractual claims, and reinsurance. Bob is the regional bad faith counsel for a major national insurer. He successfully argued to the Connecticut Supreme Court one of the leading cases involving a claim for coverage for a data-loss event under a CGL policy, Total Recall v. Federal. Bob has tried many cases to verdict in various state and federal courts. He also advises cyber and other insurers on the construction and wording of insurance and reinsurance agreements.*

Seiger Gfeller Laurie LLP *is an insurance and litigation boutique with offices in West Hartford, Connecticut, New York City, and Princeton, New Jersey. Its attorneys are admitted and regularly appear in courts throughout New England and the mid-Atlantic states. More information is available at www.sgllawgroup.com.*