D&O COMPASS

CYBER RISK

Understanding How Multiple Insurance Policies Intersect

By Bob Bregman, CPCU, MLIS, RPLU

March 2021

IRMI

IRMI D&O Compass

CYBER RISK: UNDERSTANDING HOW MULTIPLE INSURANCE POLICIES INTERSECT

by Bob Bregman, CPCU, MLIS, RPLU *March 2021*

One of the many challenges associated with cyber and privacy insurance policies is that much of the coverage these forms provide is, to some extent, *also available* within other types of insurance policies. Therefore, in addition to understanding the exact scope of protection that cyber and privacy policies make available, buyers must also concern themselves with the question of how best to coordinate their cyber and privacy policies with other policies that offer similar aspects of coverage.

The goals of this white paper are as follows.

- To describe the nature of the coverage provided by each of the various insuring agreements contained within cyber and privacy policies
- To discuss the other types of policies that provide the same or a similar scope of coverage found in these insuring agreements
- To explain how to coordinate coverage between the insuring agreements found in cyber and privacy forms *with* the comparable coverage elements contained in these other types of policies

Cyber and Privacy Insurance Policy Structure: The Insuring Agreements

The table on the following page provides an overview of the 13 most common insuring agreements contained within cyber and privacy policy forms. Note, however, that few cyber and privacy policies in the current market contain all 13. There are two reasons for this. First, different insurers often combine two (or more) of the insuring agreements noted in the table into a single insuring agreement. Second, not all insurers offer all the coverages provided by the insuring agreements noted in the table. Therefore, the typical cyber and privacy policy contains between 7 and 10 insuring agreements.

13 KEY INSURING AGREEMENTS	
Coverage Type	**Insuring Agreement**
First-Party/Post-Breach Response Coverage	1. Privacy notification and crisis management expense
Third-Party/Liability Coverages	2. Information security and privacy liability 3. Regulatory defense and penalties 4. Payment card industry fines and assessments 5. Website media 6. Bodily injury (BI) and property damage (PD) liability
First-Party/Time Element Coverages	7. Business interruption 8. Extra expense
First-Party/Direct Property Loss Coverages	9. Data assets 10. Cyber extortion 11. Computer fraud 12. Funds transfer fraud 13. Social engineering coverage

First-Party/Post-Breach Response Insuring Agreements

Cyber and privacy policies almost always contain an insuring agreement, most often titled "privacy notification and crisis management" coverage, covering the immediate cost of responding to a data breach.

Privacy Notification and Crisis Management Expense

This insuring agreement covers the direct expenses required to conduct a rapid and effective response to a data breach. Accordingly, privacy notification and crisis management coverage functions as the "loss containment" or "loss minimization" element of a cyber and privacy policy because the faster and more successfully a business reacts to a data breach, the lower the ultimate costs of that breach will usually be. In addition, since the total costs of responding to a data breach (e.g., complying with numerous notification laws) are substantial, there is also great value in having an insurance policy that provides indemnification for such costs.

The specific items covered by the privacy notification and crisis management insuring agreement include (but are not necessarily limited to) the costs related to the following.

- Hiring a *computer forensics expert* to (1) suggest measures to secure the insured's information system following a breach, (2) determine

the cause of the breach, and (3) offer advice on how to prevent future breaches. These three items are collectively referred to as "breach remediation expense."

- Engaging a *public relations firm* to assist in communicating with the public about the breach.

- Providing access to a *post-breach call center* that allows customers who inquire by telephone to receive up-to-the-minute details about the breach and learn how their personally identifiable information (PII) may have been exposed as a result.

- *Notifying affected customers* (and at times, employees) that their PII may have been compromised.

- Providing *credit monitoring* and *identity theft monitoring.* Identity theft monitoring is a service that is even more comprehensive than credit monitoring. The latter only detects situations where a bad actor attempts to open new or use existing credit lines, whereas identity theft monitoring can detect additional fraudulent uses of PII. The broadest policies provide coverage for both types of services, thus affording the insured the optimal response given the exact nature of the breach.

- *Notifying banks and credit card companies* whose credit card numbers have been accessed.

- *Most important:* This insuring agreement affords the insurer's expert assistance following the breach, often referred to as "breach coaching." Indeed, a significant rationale for buying cyber and privacy insurance is that it provides the insured with access to people who can provide immediate help to them in a crisis situation.

To place the magnitude of the costs covered by the privacy notification and crisis management insuring agreement in perspective, in its *2018 Cost of a Data Breach Study,* the Ponemon Institute reported that the average cost of responding to a data breach in 2017 was $3.86 million.

Where Else Is Privacy Notification and Crisis Management Coverage Available, and What Is the Best Strategy for Coverage Coordination? Generally, other types of insurance policies are not designed to provide coverage for privacy notification and crisis management services following a data breach. But one notable exception is the American International Group, Inc. (AIG), CyberEdge form. AIG's policy is designed primarily to cover bodily injury and property damage liability resulting from a data breach and, in effect, sits between a cyber and privacy policy and a commercial general liability (CGL) policy. (Similar coverage is also underwritten by Aegis, CFC, and Coalition.)

In addition, the CyberEdge form also provides coverage for privacy notification and crisis management expenses (with a separate insuring agreement and a separate limit). Note: coverage for bodily injury and property damage liability resulting from a data breach is discussed in more detail later in this white paper and is listed as number 6 in the "13 Key Insuring Agreements" table on page 2.

The optimal coverage coordination strategy is to amend the other insurance clause in a "standard" cyber and privacy policy so that its notification and crisis management insuring agreement functions as primary coverage. Then, if an insured has also purchased the CyberEdge (or a similar) policy, it should modify the other insurance clause so that the privacy notification and crisis management expense insuring agreement within that policy functions as excess insurance.

That said, it should be recognized that privacy notification and crisis management expenses are a uniquely "cyber" exposure. Accordingly, adequate similar coverage really cannot be found in other lines of insurance.

Third-Party Liability Insuring Agreements

As indicated in the "13 Key Insuring Agreements" table on page 2, the 5 third-party insuring agreements that may be found within cyber and privacy policies include information security and privacy liability, regulatory defense and penalties, payment card industry fines and assessments, website media liability, and bodily injury and property damage liability. Each is discussed below.

Information Security and Privacy Liability

This insuring agreement covers an insured's liability for damages sustained by a claimant as a result of a data breach, which may arise from the following.

- Loss, theft, or unauthorized disclosure of PII in the insured's care, custody, and control
- Denial of service to a customer's/third party's computer system (i.e., a denial of service attack)

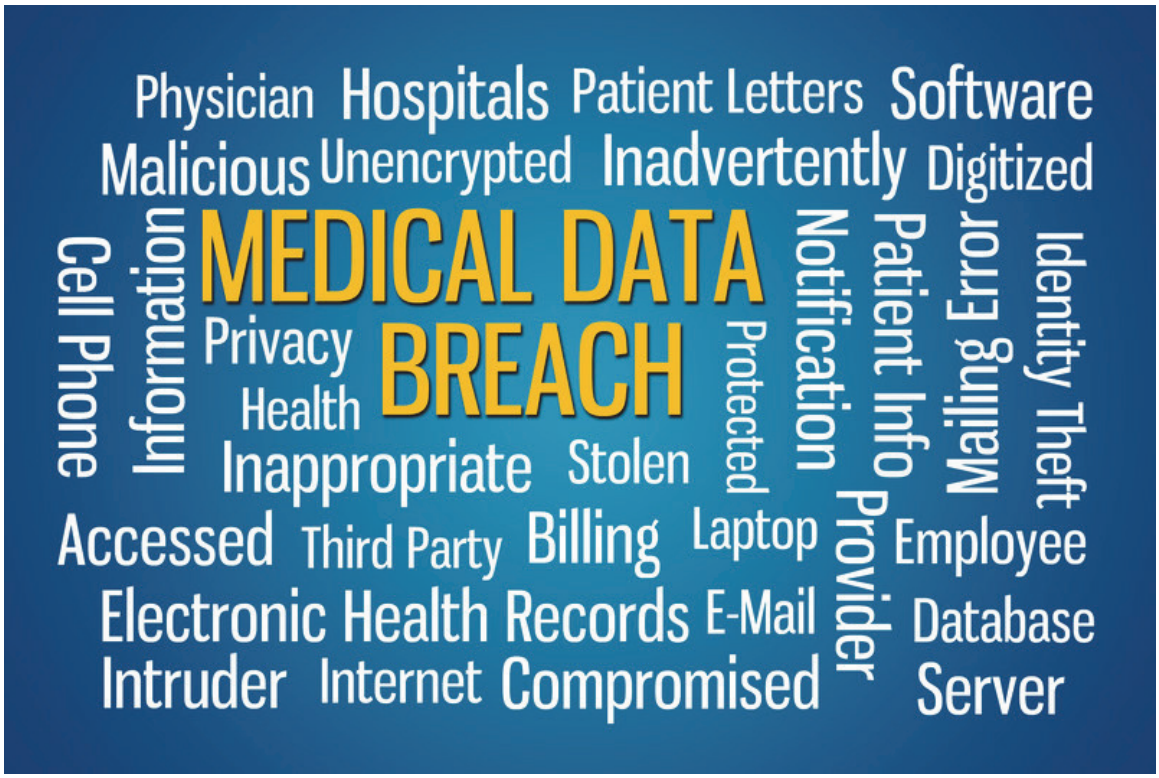
- Transmission of malicious code

- Vicarious liability in which an insured gives a third party custody of its data, which is later compromised due to the third party's negligence, and that negligence is ultimately attributed to the insured (such as when a corporation entrusts a third-party administrator with employee healthcare screening data and the administrator sustains a breach for which the employer is eventually held liable)

- Damage to or loss of data stored in the insured's computer and belonging to a third party such as a customer, client, or vendor

- Failure to timely disclose a data breach

As an example of settlements to third parties triggering the information security and privacy liability insuring agreement, on July 23, 2018, it was announced (by TV station WTVY) that Alabama-based Flowers Hospital had agreed to pay up to $150,000 to more than 1,200 people whose PII was stolen between June 2013 and February 2014 (according to a July 25, 2018, HealthITSecurity article by Fred Donovan), as part of an alleged tax fraud scheme. At the other end of the spectrum, on June 23, 2017, Anthem, Inc., an Indianapolis health insurer, agreed to a $115 million settlement resulting from a consolidation of more than 100 separate



13 CYBER TERMS TO KNOW

breach coaching: an insurer's expert assistance when an insured experiences a data breach.

denial of service attack: deliberately planned attack on a computer system or network that causes a loss of use of the computer system or network to legitimate users.

forensics: activities that take place following a data breach including securing an insured's information system, determining the cause, and preventive measures for the future.

Health Insurance Portability and Accountability Act of 1996 (HIPAA): a federal law that affords rights and protections for participants and beneficiaries in group health plans, including privacy of a patient's personal health information.

improper deep linking: linking from one website to another without permission that interferes with the intellectual property rights of the owner of the other site by using that owner's intellectual property rights to enhance the value of the first site.

malware: software that is designed to infiltrate and damage a computer system without the computer owner's knowledge or consent.

monitoring: a post-breach reviewing service conducted on behalf of the victims to watch for signs of fraudulent activity (i.e., credit monitoring).

notification: the requirement to disclose to potential victims that their personally identifiable information has been exposed to a breach.

payment card industry data security standards (PCI DSS): a set of proprietary information security protocols that businesses must follow and merchants must agree to if they accept payment from the leading credit cards.

personally identifiable information (PII): any information that can be used to uniquely identify, contact, or locate an individual, either alone or in conjunction with other sources.

ransomware: malicious software used by a hacker to block access to the insured's website by encrypting all of the victim's files and demanding a ransom payment to decrypt them.

social engineering: term for when person-to-person interaction is used to obtain good faith/voluntary access to funds or information (compare to funds transfer fraud that involves involuntary transfer).

two-factor authentication system: a method whereby a username/password and an entry code are required to access a computer system.

lawsuits involving a data breach in which the PII of approximately 78 million people was exposed, according to "Anthem Agrees To Settle 2015 Data Breach for $115 Million," by Chris Brook, Threatpost, June 26, 2017.

Where Else Is Information Security and Privacy Liability Coverage Available, and What Is the Best Strategy for Coordinating Coverage? Coverage for breaches of employee PII, as it relates to employee benefits programs (e.g., health-related data), is also found within fiduciary liability (FL) policies. Coverage for breaches of all other types of employee PII (e.g., performance evaluations) is also available under employment practices liability insurance (EPLI) policies. Admittedly, neither EPLI nor FL policies explicitly state that they cover data breaches involving employee benefits-related data. However, since EPLI policies almost always include "breach of privacy" or "invasion of privacy" as a covered peril, insurers would have a difficult time denying coverage for a data breach involving employee-related information. Similarly, as to FL policies, coverage for an employer's liability for a data breach would also seem to be available under an FL policy's "employee benefits errors and omissions" insuring agreement. This is because a data breach usually results from some form of negligence on the part of the entity that had care, custody, and control of the involved data, which is almost always the case with respect to employee benefits program data that is the subject of a data breach.

Accordingly, an insured should modify the other insurance clauses in these policies (1) so that the cyber and privacy policy functions as primary coverage for data breach-related losses involving the information security and privacy liability insuring agreement, and (2) modify the FL and EPLI policies' other insurance clauses so that these two policies apply as excess coverage for employee-related data breach losses. There are two rationales justifying this approach. First, the cyber insurer likely has more experience in handling data breach claims than does the employment practices liability insurer. Second, a cyber form's primary purpose is to cover data breaches. In contrast, breach-related privacy claims are only one of many employment benefit-related perils covered by EPLI/FL policies. Thus, the limits of these two policies should be "protected"

(by functioning as excess), so that monies will first be available to pay "garden-variety" employment/fiduciary losses.

Regulatory Defense and Penalties

This insuring agreement covers the costs of dealing with regulators who oversee state and federal data breach laws, as well as laws, such as Health Insurance Portability and Accountability Act of 1996 (HIPAA), governing protected personal health data. The two key components of this insuring agreement include (1) coverage for the costs of the legal defense required by regulatory actions, and (2) coverage for the fines and penalties that may be levied against an insured by various regulators.

Regulatory defense and penalties coverage is especially valuable because a data breach normally involves having to deal with multiple sets of regulators. This is because all 50 states have their own unique laws enumerating a business's obligations to its customers and the general public immediately following a data breach. In addition, there are a number of federal regulatory agencies that oversee data breaches, including the Federal Trade Commission, Securities and Exchange Commission, and Department of Justice. Navigating this post-breach regulatory maze requires the kind of specialized legal expertise to which most insureds do not have ready access—even if an insured has the funds to hire experienced counsel. So, by purchasing this insuring agreement, an insured will benefit from its insurer's network of data breach-related regulatory-savvy defense attorneys.

As an example of how costly data breach-related fines and penalties can be, in April 2015, AT&T, Inc., agreed to pay a $25 million penalty to the Federal Communications Commission for having exposed the PII of 280,000 of its customers, as reported in "AT&T Hands over $25 Million To Settle Data Breach Complaint," by Maritza Santillan, Tripwire, April 8, 2015. These are precisely the kinds of costs that are commonly covered (within limits) under the regulatory defense and penalties insuring agreement. In addition, breach-related penalties levied under HIPAA can also be substantial. For example, in February 2018, Fresenius Medical Care North America was fined $3.5 million under the Act in conjunction with five data breaches caused by Fresenius's failure to heed HIPAA's risk analysis and risk management rules, according to a

February 1, 2018, US Department of Health and Human Services press release.

It is also important to point out that the regulatory defense and penalties insuring agreement provides one of the few types of insurance that *affirmatively covers* fines and penalties—items otherwise considered uninsurable (and thus excluded) under virtually all other types of insurance policies.

Payment Card Industry Fines/Penalties and Loss Assessments

This insuring agreement covers contractual liability for (1) *fines and penalties* assessed against the insured (although only to the extent that such fines and penalties are insurable by law) for failing to comply with payment card industry data security standards (PCI DSS), (2) *loss assessments*, which include but are not limited to items such as the cost of replacing lost credit cards or fraud costs associated with stolen credit cards (which can often exceed the cost of fines and penalties), and (3) *defense costs* incurred in challenging assertions that the insured failed to comply with PCI DSS.

Payment card industry data security standards are a set of proprietary information security protocols that businesses must follow and merchants must agree to if they accept payment from the leading credit cards, including Visa, MasterCard, American Express, and Discover. Importantly, this insuring agreement excludes coverage for losses sustained by an insured merchant from accepting a disputed credit card transaction because this is considered a business rather than a fortuitous risk.

One of the reasons for the insurability of such fines and penalties is the fact that it is a contractual obligation assumed under a merchant services agreement. In other words, one of the provisions mandated in this agreement is the signatory's assent to subject itself to potential fines and penalties in the event it violates the terms of the agreement.

Another reason to buy payment card industry fines and penalties coverage is that, in addition to the substantial costs of fines and penalties, the loss assessments that banks incur to replace lost cards or for fraud costs from stolen cards (costs that are ultimately imposed on insureds) are often higher than the fines or penalties.

As is also the case with the regulatory defense and penalties insuring agreement, the payment card industry fines and assessments insuring agreement is also not available under any other type of policy form.

Website Media Liability

This insuring agreement covers the insured for liability incurred in conjunction with material published on its website. Such liability primarily involves three areas, as follows.

- **Personal injury.** Representative covered claims may allege invasion

of privacy, libel, slander, or defamation. An illustrative claim scenario would involve a health insurer that posts pictures of its insureds on its website without first obtaining permission, thereby producing invasion of privacy claims.

- **Commercial violations.** Lawsuits often assert that an insured engaged in infringement of copyright, trademark, or logo or plagiarism. Thus, claims may result when an insured publishes an article on its website without attributing source material appearing in the article or when an online retailer introduces its new logo that is very similar to another company's logo.

- **Miscellaneous improper Web-based acts.** Such claims are those not falling within either of the two above-noted categories. For example, a publishing firm that provides model human resources (HR) policies and procedures includes links to a page that is buried deep within an HR consulting firm's website. The consulting firm sues, alleging that the links enhance the publisher's website without benefiting the consulting firm (i.e., the consulting firm does not have the opportunity to gain revenue from advertisements that are placed on its more prominent pages and not the page that is linked to). This is known as improper "deep linking."

One oddity concerning the website media liability insuring agreement is that, unlike the other 12 insuring agreements discussed in this white paper, it covers losses that are rarely (if ever) caused by data breaches.

It should be mentioned, however, that as of 2018, an increasing minority of insurers are replacing "website media liability" insuring agreements with "full" media liability coverage that includes coverage for both "online" and "offline" media (i.e., paper publishing, broadcasting, personal appearances) as well as coverage for social media-related acts.

Where Else Is Website Media Liability Coverage Available, and What Is the Best Strategy for Coordinating Website Media Liability Coverage with Traditional Media Liability Policies? Such coverage is available as a covered peril within traditional, stand-alone media liability policies that cover all forms of media liability, including print, broadcast, and personal appearances media—*in addition to* website-related exposures. It should also be mentioned that there is often some overlap with the personal and advertising injury coverage provided by a CGL policy. Specifically, this section provides liability coverage for the insured's advertising of *its own products*—but not those of third parties. In addition, such coverage is also provided by the CGL section of a businessowners policy.

The optimal strategy is to buy a stand-alone media liability policy that covers *all*

types of media liability, including website exposures. This approach eliminates the need for an insured to purchase the website media liability insuring agreement, thus entirely avoiding the issue of coordinating coverage between the two types of policies. Although, as noted above, insureds can now obtain "full" media coverage under some insurers' cyber and privacy policies, thus eliminating their need to obtain such protection under a traditional stand-alone media policy.

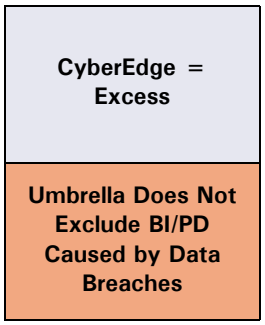
Bodily Injury and Property Damage Liability

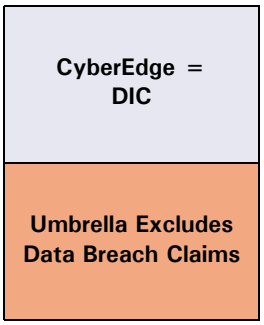
An example of a data breach causing bodily injury and property damage liability would be one in which a hacker breaches an airline's air traffic control system and uses it to bring down an airplane in a residential neighborhood. (One point to recognize is that if "terrorism" is an excluded peril in a policy, an insured could face a coverage denial in these kinds of situations.)

Coverage for data breaches that cause bodily injury and property damage liability claims is needed because (1) the information security and privacy liability insuring agreement (discussed beginning on page 4) only covers *financial losses* resulting from a data breach (and also contains an explicit bodily injury/property damage exclusion), (2) CGL policies exclude both data breach-related financial liability losses *and* bodily injury and property damage liability claims caused by data breaches, and (3) increasingly, umbrella liability insurers are excluding bodily injury and property damage liability claims caused by data breaches.

AIG's CyberEdge Policy. In 2014, AIG introduced its CyberEdge policy form, which is expressly designed to cover bodily injury and property damage liability claims caused by data breaches. Since then, Aegis, CFC, and Coalition have also begun offering this coverage. (As discussed earlier in this white paper, the AIG CyberEdge policy also contains a separate insuring agreement covering notification and crisis management expenses.) Another key coverage aspect within the CyberEdge policy is that it provides coverage on *both* a difference-in-conditions (DIC) and an excess basis.

- **Two examples.** An insured has an umbrella policy that does not exclude bodily injury and property damage claims caused by data breaches. In this instance, the CyberEdge policy would provide coverage on an excess basis after the umbrella policy's limits are exhausted. In the case of an umbrella





that excluded data breach claims, the CyberEdge policy would drop down over the coverage gap created by the exclusion and provide coverage on a DIC basis.

Where Else Is Data Breach-Related Bodily Injury and Property Damage Liability Coverage Available? Nowhere. It is yet another type of policy that provides a unique form of coverage.

First-Party/Time Element Insuring Agreements

Cyber and privacy insurance policies provide two types of time element insuring agreements: business interruption (BI) and extra expense (EE) losses. Many insurers do not offer time element coverages because, philosophically, they view cyber and privacy insurance as a liability/third-party coverage rather than a property/first-party coverage. Other underwriters offer these two time element insuring agreements but by endorsement rather than within their standard policy. Finally, a crucial point is that, under all cyber insurers' time element insuring agreements, coverage is triggered only by an "electronic disruption" or a "failure of computer security." On the other hand, there is no coverage for time element losses caused by the physical damage perils for which coverage is available (or could have been arranged) under the commercial property insurance program (e.g., fire, explosion, windstorm, flood, and earthquake). The rationale for this approach is that, if a computer system is disabled by these kinds of perils and a BI/EE loss results, coverage is available (or could have been arranged) under standard property insurance policies.

Recently, however, some insurers have broadened their time element insuring agreements to also include coverage for "system failures" that encompass unplanned and unintended outages of a computer system that *are not* breach related, such as an insured's unintentional or accidental error in modifying, creating, handling, or maintaining data or computer systems. Such coverage contrasts with "traditional" BI coverage under a cyber and privacy policy, which is triggered by outside intrusions (i.e., hacking, data theft, or malware). This is a valuable coverage extension because "system failures" are almost always excluded by standard property insurance policy forms.

Business Interruption

This insuring agreement covers loss of income incurred during the "period of recovery" resulting from an "electronic disruption." Virtually all insurers' versions of the BI insuring agreement cover *income loss* during the period in which an insured's business is unable to operate, such as when (as a result of a data breach) an online retailer must shut down for 3 days, cannot take orders for its products, and consequently loses sales revenue during this period of time. However, there are significant differences in the length of

the period of recovery offered by different insurers. For instance, the broadest policies provide coverage for as long as 180 days following an "electronic disruption," whereas other forms limit coverage to as few as 30 days.

In addition, some insurers' business interruption insuring agreements also encompass coverage for an *extended period of indemnity,* whereby coverage continues even after operations resume and does not cease until sales return to prebreach levels up to a specified maximum number of days following the "electronic disruption."

More and more frequently, some cyber forms also cover dependent business interruption in order to protect insureds from scenarios in which one of their vendors or suppliers incurs some form of cyber-related downtime and cannot deliver services to the insured as expected.

Extra Expense

This insuring agreement covers *additional* costs that a business incurs in an effort to expedite its return to regular operations following an "electronic disruption" or "systems failure." Such costs may include (but are not limited to) overtime labor, express parts shipping, and the cost of hiring (and transporting to its premises) special experts. Under some policies, EE coverage applies *only* if the extra expense actually reduces the loss (i.e., hastens a firm's return to operations), whereas under other underwriters' versions of this insuring agreement, the insurer will cover the extra expenses incurred, even if they do not actually expedite an insured's return to full operating capacity. Another variation of the EE insuring agreement that is offered by some insurers covers extra expenses required to maintain operations following a data breach, even if there is a negligible loss of income resulting from the outage. Coverage of this kind would be essential for insureds that must maintain continuity of operations, such as a school or university.

Some insurers "bundle" BI and EE coverage under a single insuring agreement, and others separate them; still others offer BI but not EE coverage.

Both BI and EE insuring agreements are usually (but not always) subject to a "time" deductible (rather than a "dollar" deductible) before coverage applies—most often 8, 12, or 24 hours. In contrast, the other 12 insuring agreements discussed in this white paper are subject to a dollar deductible.

Where Else Is Business Interruption and Extra Expense Coverage Available, and What Is the Optimal Coverage Coordination Strategy? Standard property insurance forms provide only very limited coverage for losses from "electronic disruptions." Specifically, a standard commercial property policy that provides business income and extra expense coverage has a

built-in limit of just $2,500 for loss from an interruption of computer operations. In addition, electronic data processing (EDP) policies typically impose sublimits on the coverage for loss from a computer virus that are very low in relation to the other policy limits and in relation to the loss exposure. Loss due to computer hacking in which there is no damage to data may or may not be covered.

Cyber and privacy policies should be endorsed to cover business interruption on a primary basis, with the commercial property and EDP policies endorsed to cover this exposure on an excess basis. Clearly, given their low limits, commercial property or EDP policies cannot be relied on as a robust source of cyber-related time element coverage. Moreover, neither of these two policies provides extra expense coverage for data breaches.

First-Party/Direct Property Loss Insuring Agreements

The five insuring agreements covering first-party/direct property loss are those applying to data assets, cyber extortion, computer fraud, funds transfer fraud, and social engineering, which are discussed below.

Data Asset Coverage

This insuring agreement covers the cost of *restoring* and *recovering* the data lost from the "failure of an insured's computer security" (and in some instances, as mentioned on page 12, for "systems failure"). A loss scenario under which this insuring agreement applies may involve a hacker introducing a virus into the systems housing an insured's customer database, and the virus appears to delete

the data from the company's computer system. In this instance, the data asset insuring agreement pays the cost of restoring the lost customer databases. Under some forms, restoration entails recovery by "electronic means" only, rather than any actual research to recover lost data assets. However, more recently, insurers have broadened their forms to also cover the cost to recreate lost data by recovering the data from paper records. Nor does this insuring agreement cover security or antivirus software upgrading (since the lack of up-to-date software is often the cause of a data asset loss).

Where Else Is Data Asset Coverage Available, and What Is the Best Strategy for Coordinating Data Asset Coverage with These Policies? Data asset coverage under a standard commercial property policy is restricted to the limit that applies under the electronic data additional coverage, which is just $2,500 unless a higher limit is shown. Data asset coverage under EDP policies is provided subject to the policy's sublimit for computer virus, which is typically relatively low in relation to the other policy limits and the loss exposure.

Given the paucity of data asset coverage within commercial property and EDP policies, the optimal coordination strategy is to make the cyber policy primary as respects coverage for data assets, and any commercial property coverage or EDP coverage should apply as excess.

Cyber-Extortion Coverage

This insuring agreement covers loss sustained from computer-aided extortion. A typical covered claim involves an insured being victimized by "ransomware." In this situation, a hacker uses malicious software to block access to the insured's website by encrypting all the victim's files and demanding a ransom payment to decrypt them.

This insuring agreement covers the following.

- Monies paid to meet extortion demands
- Forensics, including fees paid to computer security experts who advise the insured on how to prevent future extortion attempts
- Costs incurred for expert assistance in negotiating with such extortionists

Obtaining the help of experts to negotiate with the extortionists may be the most important coverage component of all, since few businesses have the expertise to deal successfully with ransom demands of this nature. Moreover, experts who deal regularly with ransom seekers will often be successful in negotiating a vast reduction from initial demand to the actual, final ransom payment.

Where Else Is Cyber-Extortion Coverage Available, and What Is the Optimal

Coordination Strategy? Cyber-extortion exposure is also covered under kidnap and ransom (K&R) policy forms (a.k.a. "special crime" policies). Coverage may also be available under an extortion endorsement to a commercial crime policy.

The optimal coordination approach is to endorse the cyber policy's "other insurance" clause so that it pays cyber-related extortion expenses on a primary basis and endorse the K&R/computer extortion policy(ies) so that it (or they) will pay on an excess basis. This approach protects the K&R policy's limits, making them available for "garden-variety" extortion attempts (e.g., ransoming an executive or responding to a threat to damage a manufacturing plant). Another reason to have the cyber policy cover cyber-related extortion events on a primary basis is that the forensics provided by cyber insurers tend to be more extensive than what is made available by K&R or commercial crime insurers.

Computer Fraud Coverage

This insuring agreement covers loss from fraudulent, unauthorized entry into a computer system, resulting in a theft of money or securities. A representative computer fraud loss would involve a hacker accessing a person's brokerage account by stealing the individual's username and password and then transferring money from that person's account to the hacker's account at the same brokerage.

Funds Transfer Fraud Coverage

This insuring agreement covers loss sustained when funds are fraudulently *transferred* from one financial institution to another. A representative loss scenario would involve a situation in which a hacker infiltrates a European bank's computer system, using it to electronically transfer $5 million to her bank in the Caribbean. By the time the bank realizes what has happened, the hacker has withdrawn the funds from her bank in the Caribbean and absconded with the $5 million in cash.

Funds Transfer Fraud versus Computer Fraud: What's the Difference? The difference between the application of coverage under the funds transfer fraud and computer fraud insuring agreements is that computer fraud does not involve the *transfer* of monies *between* financial institutions, whereas funds transfer fraud does.

ALTERNATIVE SOURCES OF COVERAGE FOR THE 13 KEY INSURING AGREEMENTS		
Coverage Type	**Insuring Agreement**	**Coverage under Other Policy**
First-Party/ Post-Breach Response Coverage	1. Privacy notification and crisis management expense	AIG CyberEdge policy
Third-Party/ Liability Coverages	2. Information security and privacy liability	Employment practices liability, fiduciary liability (for employee privacy liability exposures only)
	3. Regulatory defense and penalties	None
	4. Payment card industry fines and assessments	None
	5. Website media	Traditional media liability policy, CGL policy (personal and advertising injury coverage)
	6. Bodily injury and property damage liability	Umbrella policy
First-Party/ Time Element Coverages	7. Business interruption 8. Extra expense	(a) Commercial property policy (subject to interruption of computer operations limit of $2,500) (b) EDP policy (subject to computer virus/hacking sublimit) (c) Factory Mutual forms
First-Party/ Theft of Property Coverages	9. Data assets	(a) Commercial property policy (subject to electronic data limit of $2,500) (b) EDP policy (subject to computer virus/hacking sublimit)
	10.Cyber extortion	(a) K&R policy (b) Extortion endorsement to commercial crime policy (no forensics/negotiating assistance)
	11. Computer fraud	Commercial crime policy
	12. Funds transfer fraud	Commercial crime policy
	13. Social engineering coverage	Endorsement to commercial crime policy

Social Engineering Coverage

This insuring agreement covers losses of funds that are transferred by means of "fraudulent instructions." A representative loss would involve a chief financial officer (CFO) receiving an email appearing to be from his company's treasurer, requesting that the CFO transfer $50,000 to one of the banks at which the company has an account. The CFO follows the treasurer's instructions, but instead of being transferred to the company's bank, the $50,000 ends up in the bank account of the cyber thief, whose fraudulent email "impersonated" an email that would typically come from the treasurer.

Social engineering coverage within cyber forms is usually written with a number of restrictions: (1) limits are rarely available above $100,000, (2) coverage always applies excess of any applicable commercial crime policy, and (3) the insured's computer system must use a "two-factor" authentication system (i.e., username/password *and* an entry code that is periodically texted to the user of the email system).

Social Engineering Coverage versus Funds Transfer Fraud Coverage: What's the Difference? Social engineering coverage involves a *good faith*/*voluntary* transfer (usually prompted by an email or oral instruction). In contrast, funds transfer fraud coverage applies to *involuntary* transfers of funds, usually by means of an unauthorized intrusion into a computer system. In the social engineering loss scenario above, the CFO transferred the funds based on the good faith assumption that the email he received requesting the transfer was from the company's treasurer. Conversely, in the funds transfer fraud loss example, there was no good faith transfer of funds. Rather, the hacker fraudulently accessed the bank's computer system and then used the system to transfer monies to her Caribbean bank.

Where Else Are Computer Fraud, Funds Transfer Fraud, and Social Engineering Coverages Available, and What Is the Optimal Coverage Coordination Strategy? A majority of cyber and privacy insurers avoid providing these three types of theft of property coverages. This is because the losses they address can be readily covered under commercial crime policies (which offer separate insuring agreements for these three exposures). In fact, limits of $1 million (and higher) are frequently available for the computer and funds transfer fraud coverage since it is very common for the computer and funds transfer fraud limit to be the same as the limit that applies to employee theft. The limit for fraudulent impersonation coverage is usually significantly lower than the computer and funds transfer limit. In contrast, cyber insurers do not generally offer limits higher than $100,000 for these three insuring agreements, if they are offered at all.

Accordingly, for many insureds, especially financial institutions, there may be no need to even buy these three insuring agreements under a cyber and privacy pol-

icy. Rather, such businesses should consider obtaining these three insuring agreements under a commercial crime policy. On the other hand, businesses that do infrequent wire transfers (and for small amounts) may be better served by obtaining these three coverages (assuming they are made available) under their cyber and privacy policy, rather than under a commercial crime policy.

The table on page 17 summarizes the alternative sources of coverage for the 13 insuring agreements discussed within this article.

Robert Bregman, CPCU, MLIS, RPLU
International Risk Management Institute, Inc.
www.IRMI.com

Bob Bregman began his insurance career in 1976 and was an IRMI research analyst from 1989 until his retirement in 2019. He is the principal author of IRMI's *Professional Liability Insurance* reference manual, edited IRMI's *D&O MAPS* and *Employment Practices Liability Consultant (EPLiC)* publications, and is the author of IRMI's Management Liability Insurance Specialist (MLIS) certification program. More information about Mr. Bregman can be found in the About IRMI section of www.IRMI.com.