35+ YEARS IN PUBLICATION

ADJUSTINGTODAY®

Adjusters International Limited

## FROM THE EDITOR

The devastating impact of recent headline-making cyber-losses serve as a warning to all businesses. Our reliance on technology makes us very vulnerable. Businesses must better understand cyber risks in order to properly insure against cyber-losses as well as consider hiring professionals when making cyber-claims.

In June 2024, CDK Global, a software provider to automobile dealerships, suffered a cyberattack. The attackers held CDK Global hostage, demanding a ransom to release the software. This paralyzed over 15,000 automobile dealerships in North America for over two weeks. The Anderson Economic Group estimates the losses to the impacted dealerships will exceed 1 billion dollars. According to CNN.com's estimations, cybercriminals extorted over $1.1 billion in ransom payments in 2023.

Only one month later, CrowdStrike, a provider of security software designed to protect against cyberattacks, distributed a faulty update – resulting in the largest IT outage in history. While the problem was resolved in a few hours, an estimated 8.5 million systems crashed resulting in more than $10 billion in losses. Airports, banks, hotels, hospitals and government services were among the hardest hit.

*continued on next page »*

# Segregating Cyber Coverage

***Adjusters may have to resist demands to end "silent cyber" coverage***

*By Joseph S. Harrington, CPCU*

Back in 2016, the Claims & Litigation Management Alliance made this prediction in a report provided at its Cyber Liability Summit:

***"The cyber claims adjuster's role will transform beyond data breach and expand into new technology-based claims, including those traditionally reserved for other insurance policies, such as property and bodily injury . . .***

***"The growth of cyber insurance into new spaces will assuredly lead to situations in which multiple policies respond to the same claim. It is critical that early in the claims process the adjuster work with the insured to identify all policies that may cover the claim . . "[1]***

Not long after that, however, insurers began a concerted effort to make sure that multiple policies would **not** respond to the same claim - if the claim involved some sort of "cyber" peril or loss.

Increased business automation has resulted in a substantial increase in cyber-risks for all businesses, large and small. According to *Allianz Risk Barometer 2024*, cyber-incidents are the primary global risk, surpassing business interruption and natural catastrophes, which are second and third respectively. Businesses are at great risk of loss should any of the systems they rely on fail.

These events highlight the need for businesses to purchase cyber-insurance *and* understand how to use it. All insurance policies are complex, but cyber-policies take things to a new level. For example, insurance policies have defined terms that dramatically change how the policy is to be interpreted and applied. The Insurance Services Offices (ISO) – the nation's leading property/casualty advisory organization – lists only three defined terms on its business and personal property form. In comparison, ISO's cyber-coverage form has 25 defined terms. And the most common cyber insurance policies in use often have over 100 defined terms.

Understanding how to apply the terms of a cyber-policy to cyber-related event is best left to an experienced team of professional trusted advisors. The insured's broker, attorney, accountant, risk manager and public adjuster bring valuable knowledge and experience to the process. Failure to properly identify goals, strategize and submit a cyber-claim that doesn't meet the conditions of the cyber-policy might well prevent a full recovery.

Of course, the first step in protecting against cyber-risk is having a comprehensive cyber-insurance policy. This issue of *Adjusting Today* examines the evolution of cyber-coverage, from the now-eliminated "silent-cyber" coverage to the current cyber-policies. It also addresses the multitude of risks that may be covered under these policies, including crime, liability, property – and even media and reputational harm. This article provides practical information that is useful in navigating the ever-changing world of cyber-risks. Enjoy!

**Ethan A. Gross, JD**
*Editor*

**The 'silent cyber' problem**
"Silent cyber" refers to losses arising from "cyber perils" that might be covered under property and liability policies that were never intended, written, or priced to cover such losses. Cyber perils include, under various labels:

- **Hacking:** A unauthorized intrusion into a computer network, constituting a "breach" of information stored on the network - even if the information is not accessed, stolen, or used.
- **Social engineering:** Schemes to trick legitimate system users into transferring funds, providing confidential information, or allowing access to unauthorized individuals.
- **Denial of service:** The use of malicious coding ("malware") or other means to prevent an organization from accessing its own systems and/or data.
- **Cyber extortion:** Demands for money in exchange for restoring access to compromised systems and/or data.

In addition to these intentional threats to data and networks, cyber risks also entail losses arising from accidental data compromises and unintentional transmission of computer viruses.

In 2019, the Lloyd's Market Association (LMA) issued a directive to its members to eliminate "silent cyber" coverage in non-cyber policies. The direction was prompted by regulators in the United Kingdom.

LMA directives have great influence on global insurance markets, especially among non-admitted carriers who underwrite most cyber-insurance. Led by Lloyd's, insurers throughout the world are striving to restrict coverage for "cyber-events" to policies providing "affirmative" cyber-coverage that is specifically written and rated to address cyber-hazards.*

**Auto risk analogy**
Efforts to eliminate "silent" cyber coverage and establish "affirmative" cyber coverage reflect reasoning that considers cyber perils as distinctly different from risks insured by

traditional property and liability policies. To illustrate, consider the well-established distinction between auto risk and other risks faced by a household or commercial enterprise.

Driving vehicles on public roads poses distinctly different activities and hazards from those encountered at properties. Therefore, road vehicles are among the types of property not covered under standard homeowners and commercial property policies. Similarly, homeowners and commercial liability policies exclude coverage for bodily injury or property damage arising from the ownership or use of autos. Vehicles are insured separately under auto policies written and rated for the hazards of the road.†

Property/casualty insurers are seeking to establish a similar distinction between cyber risk and other types of risk. There are, indeed, several parallels between cyber risk and auto risk:

- Both cyber and auto risk arise from activities that, at least at one time, were distinct from other insured activities. It is still not uncommon for organizations to outsource all or most of their transit and systems operations.
- The principal causes of auto and cyber loss are distinctly different from those of property and liability losses, and the methods for controlling those losses are also different.
- The principal risk factors driving auto and cyber losses — driver quality and systems management — are shared across sectors and less dependent on specific hazards at an insured location.

Simply put, there are risks associated with what you do and where you do it. Then there are risks associated with the vehicles and automation you use to do it — which may or may not be your own.

Under this logic, computer data and network functionality are distinct forms of intangible property that exist separately from tangible property - even from the computer hardware on which they reside. These "digital assets" are typically limited to data, software, functionality, and related intellectual property rights, as well as potential damage to one's reputation, financial loss, and legal liability resulting from the failure to safeguard sensitive information.‡

**ISO's approach**

The Insurance Services Office (ISO) is the United States leading property/casualty advisory organization. In 2019, ISO introduced general liability endorsements that exclude coverage for bodily injury, property damage, and personal-advertising injury arising from:

(1) "Access to or disclosure of any person's or organization's confidential or personal information."

(2) "Loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data."

There are three versions of the exclusion in ISO general liability programs:

- One with an exception preserving coverage for bodily injury claims.
- One applying the exclusion to personal-advertising injury claims only.
- A total exclusion with no exception for any type of claim.

ISO later developed "cyber incident" exclusions in its commercial property programs. These endorsements exclude coverage for first-party losses arising from:

(1) "Unauthorized access to or use of any computer system," "a virus or other malicious or harmful code."

(2) "A denial-of-service attack that disrupts, prevents, or restricts access to or use of any computer system."

There are two basic versions of the cyber-incident property exclusion. Both include an exception preserving coverage under basic policy limits for damage due to fire and explosion resulting from a cyber incident. One of them provides an additional exception under separate scheduled limits for ensuing damage due to other covered perils. (**Note:** The exclusions do not apply to built-in additional coverages for electronic data and interruption of computer operations, or to optional coverage for electronic commerce.)§

ISO also has a program of cyber-insurance forms and loss costs, but plays less of a defining role in cyber-insurance than in other lines. While

provisions vary from carrier to carrier, cyber policies often have exclusions for physical damage to the insured's property, as well as liability exclusions for bodily injury, third-party property damage, professional liability, management liability, and other exposures traditionally insured under other policies.

**Core operations**

Compared to auto risk, cyber risk is now much more integrated into the core operations of commercial enterprises and, increasingly, households. To be sure, IT design and maintenance can still be outsourced, but as long as insureds use computer networks to carry out daily activities, it's virtually impossible to segregate all cyber exposures from other types of exposures.

Indeed, with the integration of artificial intelligence and remote sensors communicating through the "Internet of Things" (also known as smart objects), operating decisions are increasingly made without direct human intervention. For instance, a network might operate your lights when you're away from home and adjust the thermostat as you head home. In the workplace, networks monitor pressure within manufacturing equipment, automatically route shipments, monitor medical patient health, and much more.

> ***Simply put, there are risks associated with what you do and where you do it, then there are risks associated with the vehicles and automation you use to do it — which may or may not be your own.***

- If temperature sensors fail because they are hacked and a fire results from overheated equipment, where does the cyber loss end and the fire loss begin? How could you tell in a smoldering ruin?
- What type of loss is it if a GPS app is disabled or manipulated to misdirect a shipment into the hands of cargo thieves?
- If a professional utilizes artificial intelligence in decision-making and it turns out that certain information was corrupted, how do you deduct the cyber share of resulting losses from losses attributable to professional liability? Similarly, how does one distinguish between a public company's cyber loss from a ransomware attack and the liability of directors and officers for allowing the attack to happen?

In light of questions like these, attorneys for Anderson Kill, a prominent law firm that advocates for insureds, attempted to clarify the issues. They argued that whatever cyber-related exposures are excluded from other policies should be shifted to more expansive cyber policies. In 2019, they wrote:

***"If insurance companies begin a concerted effort to remove 'silent' coverage for cyber-related claims from policies protecting against bodily injury, property damage, first-party property [loss], business interruption, maritime and marine cargo insurance claims, then that protection will need to be found under cyber policies that provide more robust coverage than is presently the norm."***[2]

Five years later, there is little indication that cyber policies are being extended to cover such claims. One key exception is the recent introduction of contingent coverage for bodily injury and property damage liability in some cyber policies.

**Cyber premium and provisions**

From the mid-2010s until recently, there has been soaring growth in the amount of premiums derived from cyber coverage written on stand-alone policies. Growth in premiums derived from "packaged" cyber coverage — provided in conjunction with other coverage (i.e., businessowners policies) — is slower.

The percentage of cyber premiums derived from

stand-alone, cyber-only policies grew to account for more than two-thirds of the US domestic cyber insurance market from 2022. That trend reversed slightly in 2023, when premiums for stand-alone cyber policies *decreased* by about three percent. Meanwhile, premiums actually rose by slightly more than five percent for packaged cyber. It remains to be seen whether the shift to packaged cyber coverage in 2023 was a blip or a sign of something more permanent. There's little doubt, however, that insureds will seek coverage for a claim wherever they think they can find it.

The unique nature of cyber risk is reflected in the unique structure of cyber policies.

Most property and liability policies consist of one to three major insuring agreements, subject to per loss and aggregate limits, with some additional or supplemental coverages with sub-limits provided within or in addition to the basic policy limits.

Cyber policies commonly have multiple insuring agreements (the ISO model has six) addressing first-party losses, third-party liability, and additional costs arising from a cyber event. In most cases, loss settlement is based on an ascending scale of limits:

- A sublimit for each insuring agreement, which is subject to—
- A per-loss limit for a cyber event (typically defined to include a related series of incidents); which in turn is subject to—
- An aggregate policy limit.

There may also be additional sub-limits under each insuring agreement for different types of attacks, failures, or costs associated with an insuring agreement.

Cyber claims specialists must apportion claim costs among various insuring agreements to achieve the maximum possible recovery. This may require forgoing a claim under one insuring agreement in order to claim the maximum available under another while staying within the per-loss and aggregate limits.

**Covered or excluded?**
GBA Insurance, a brokerage based in Scarsdale, NY, identifies seven types of cyber-related exposures for which insureds will want to know where to look for coverage[3] *(see chart on page 7)*.

**Overlap Examples**
Consider an account that has a cyber policy with media liability coverage that extends to advertising injury and a commercial general liability (CGL) policy with coverage for personal and advertising injury. Presume also that the CGL limit for the personal/advertising injury is more than the amount provided under the cyber media liability coverage.

Other considerations aside, if the CGL policy has no cyber exclusion, the insured would seek coverage for a cyber-related advertising injury claim under it. CGL policies provide more coverage and typically pay defense costs outside policy limits. Also, filing the claim under the CGL policy reserves coverage under a cyber policy's per loss and aggregate limits for claims under other


insuring agreements.

If the claim is subject to a CGL cyber exclusion, the insured could still lodge the claim under the cyber media liability coverage. Before doing so, however, an adjuster would still have to determine whether invoking the media coverage would allow for the maximum possible recovery under the cyber policy or deplete the per-loss and aggregate limits in a way detrimental to the insured.

**Coverage gaps**

The example above describes overlapping coverage, which insurers consider to be a problem to be solved by segmenting cyber risk from other exposures.

Insureds and their adjusters are more concerned about coverage ***gaps***, especially in cases where there are two policies. Each policy might be expected to cover a loss, combining to eliminate coverage by virtue of complementary exclusions:

- Cyber exclusions in property and liability policies, and
- Cyber policy exclusions for physical damage and/or general, professional, or management liability.

If a cyber event contributed to a bodily injury (e.g., by interfering with machinery) the policyholder could be without coverage. For example, if the CGL policy has a cyber exclusion and the cyber policy has an exclusion for bodily injury claims. Both of those types of exclusions are still quite common, even as some cyber insurers have begun adding contingent bodily injury and property damage coverage.

There's even greater potential exposure in professional and management liability.

"Some companies still operate under an assumption that coverage [for cyber events] will be afforded under the professional liability or directors & officers insurance policies," writes

GBA Insurance, cited above.[4] On the contrary, GBA identifies several "potential exit points" for carriers to avoid professional and management liability claims. Apart from explicit cyber exclusions, these "exit points" include professional services and product defect exclusions. Plus there is broad exclusionary language in provisions addressing terrorism, privacy violations, infringement of intellectual property, and contractual liability.

As a broker, GBA advises buyers to negotiate — when possible — for eliminating these exclusions or limiting their scope, particularly by narrowing their "lead-in" language. That is, insureds are advised to avoid extended phrases such as "for, based upon, arising from, in consequence of, or related to" in favor of shorter, more targeted language for applying an exclusion.

Regarding first-party property coverage, insureds who suffer ensuing physical damage from a cyber incident (other than by fire or explosion) could be left without coverage if their ISO-based property policy excludes coverage for such losses. Given that, if a cyber policy does not explicitly exclude coverage for physical damage to property, an adjuster will explore whether coverage is available under that policy.

**Underlying liability**

On the liability side, an adjuster will look beyond cyber exclusions in liability policies to seek coverage for the underlying liability.

| Type of claim (identified by GBA Insurance) | Potentially applicable coverage provisions (provided by author) |
|---|---|
| Website accessibility claims (by individuals unable to utilize a website because of a personal disability) | • May or may not fall under policy definitions of insured injury or damage<br>• May be subject to exclusions for violations of the Americans with Disabilities Act |
| Breaches of employee privacy | • May be subject to cyber exclusions in employment practices policies, or vice versa |
| Media liability | • Commonly covered under cyber policies, but only for non-media companies<br>• May be eligible for CGL personal and advertising injury coverage |
| Cyber related investor claims and regulatory actions | • May be subject to securities exclusions in cyber policies and cyber exclusions in D&O policies |
| Computer failure/breakdown | • Some, but not all, cyber policies cover failures in hardware and systems<br>• May be subject to mechanical breakdown exclusions in property policies<br>• May be covered under equipment breakdown policies |
| Computer and funds transfer fraud | • Frauds committed through cyber means commonly covered under cyber policies<br>• Coverage generally available under commercial crime policies |
| Cyber-instigated liability for third-party bodily injury and property damage | • May be subject to CGL cyber exclusions<br>• May be covered under contingent bodily injury and property damage coverage now starting to appear in cyber policies |

For example, one would not expect a cyber policy to cover a professional liability claim simply because faulty guidance was communicated by email. But what if a professional service uses a client's electronic network to gather information and communicate with the client? What if a loss results from a miscalculation or miscommunication due to a cyber peril?

Such cases are growing rapidly. Where does one draw the line between the cyber exposure and, in these cases, a professional liability exposure? Even if it can be demonstrated that a computer system malfunctioned to produce the loss, there still be potential liability for a professional's selection and implementation of the system.

Let's turn this on its head and presume that a management or professional liability policy is written with an exclusion of coverage for any loss caused by or arising from a cyber-attack, data breach, or another of the common "cyber perils." The law will still find liability if claimants can prove negligence or a wrongful act. The only question will be what, if any, coverage is triggered by the claim.

As cyber-insurance evolves, cyber adjusters — and property and liability adjusters — will have to become "jacks of all trades," as the CLM suggested back in 2016. Their work will become more complicated as carriers seek to enforce a separation between cyber and non-cyber risks that may not be possible or practical.

The growing prevalence of cyber threats underscores the urgent need for businesses to take proactive steps in safeguarding their operations. The devastating impacts of cyber-attacks, like those involving CDK Global and CrowdStrike, serve as cautionary tales for all organizations that rely on technology. As these incidents illustrate, no business — large or small —is immune to the paralyzing effects of cyber perils. Therefore, it is imperative for organizations to adopt a multi-faceted approach to managing cyber risks, combining robust insurance coverage with a deep understanding of how to navigate the complex landscape of cyber policies:

- **Invest in Comprehensive Cyber-Insurance Policies:** Given the rapid evolution of cyber-attacks and their devastating financial consequences, businesses must prioritize obtaining comprehensive cyber-insurance policies. As cyber-incidents have now surpassed traditional risks like business interruption and natural catastrophes, insurance coverage needs to evolve accordingly. Silent cyber exclusions, while intended to delineate traditional and cyber risks, create significant coverage gaps. Businesses must seek out cyber policies that address a wide range of exposures, from financial crime and data breaches to property damage and reputational harm. Organizations should also ensure their cyber policies are tailored to their specific risk profile. Coverage gaps must be addressed by developing policies that include affirmative coverage for all cyber-related risks, such as third-party bodily injury and property damage. Doing so will mitigate the risk of catastrophic losses, which could otherwise fall outside the scope of traditional property and liability policies.
- **Engage a Professional Team to Navigate Cyber Claims:** The complexities of cyber-insurance make it crucial for businesses to involve trusted professionals when filing cyber-related claims. The importance of assembling a team that includes a broker, attorney, risk manager, and public adjuster to

> ***Some companies still operate under an assumption that coverage [for cyber events] will be afforded under the professional liability or directors & officers insurance policies.***

ensure the insured receives full recovery under their policy cannot be overstated enough. These professionals possess the expertise to interpret the often intricate terms of a cyber policy, which can contain over 100 defined terms, compared to just a handful in traditional policies. In a landscape where cyber policies are still evolving, having a knowledgeable advocate on your side can make all the difference in obtaining the full recovery your business needs to bounce back from a cyber event.

- **Enhance Cybersecurity Practices:** While insurance coverage provides an essential safety net, it should never be viewed as the only defense against cyber threats. As businesses become more reliant on interconnected systems, automation, and artificial intelligence, the potential attack surfaces for cybercriminals grow exponentially. The integration of the Internet of Things, smart technologies, and AI-driven decision-making has transformed the way businesses operate, but it has also introduced new vulnerabilities. Hackers can exploit these interconnected systems to create massive disruptions that lead to outages across critical industries. To minimize exposure to cyber-attacks, businesses must implement and continuously upgrade their cybersecurity infrastructure. By maintaining strong security practices, businesses will not only reduce their likelihood of falling victim to cybercrime but will also be in a stronger position when filing a cyber-insurance claim, as many policies require evidence of reasonable efforts to prevent breaches in order to qualify for full coverage. In this way, enhancing cybersecurity practices is not just a preventative measure but also a crucial element in ensuring a successful insurance recovery when incidents do occur.
- **Prepare for the Future of Cyber Risk:** As the cyber insurance market continues to evolve, businesses must remain agile. Recent trends, such as the growth of packaged cyber policies,

indicate that insurers are constantly adjusting their offerings to meet the changing threat landscape. It is essential for organizations to stay informed about these developments and adjust their coverage as needed.

The path forward requires a comprehensive approach that combines proper insurance, expert advice, and proactive risk management. As the digital landscape evolves, so too must the way individuals, businesses, and insurers prepare for and respond to cyber threats. No longer can organizations rely on traditional property or liability policies to provide implicit coverage for cyber-related incidents. The shift from "silent cyber" to "affirmative cyber" policies reflects an industry-wide recognition that cyber risks are distinct, multifaceted, and constantly evolving.

The risks posed by cyber perils, such as ransomware, denial-of-service attacks, and social engineering schemes, are too significant to be ignored. As these threats increase in complexity, organizations must take a more holistic approach to risk management. This includes actively assessing where coverage overlaps and gaps exist across multiple insurance policies.

Cyber threats can trigger claims that blur the lines between cyber, property, liability, and even professional indemnity coverage, requiring policyholders to carefully review policy terms, exclusions, and sub-limits.

The need for proactive risk management has never been greater. Organizations must implement robust cybersecurity measures, regularly review their insurance coverage, and work with insurance professionals to address any gaps. As the concept of "digital assets" grows in importance, so too does the need for policies that explicitly protect them. Just as auto insurance separates road risk from home and business risk, insurers are striving to carve out clear definitions for cyber risks. By embracing this proactive, multi-layered strategy, individuals and businesses can build resilience against both known and unforeseen cyber threats. While the cyber threat landscape will continue to change, a thoughtful combination of sound insurance coverage, risk management, and expert guidance will remain the most effective way to safeguard operations, assets, and long-term viability.

# Cyber & Non-Cyber Liability Coverage

| Exposure | Cyber Policy Coverage | Coverage Under Other Policies |
|---|---|---|
| Liability for bodily injury to a third party | Not commonly covered, but contingent coverage is starting to spread | Covered under CGL policy, but may be subject to cyber exclusion |
| Liability for physical damage to property of a third party | Not commonly covered, but contingent coverage is starting to spread | Covered under CGL policy, but may be subject to cyber exclusion |
| Liability for personal and advertising injury to a third party | Covered under a "media liability" or equivalent limit, but only if one is indicated. | Covered under CGL policy, but may be subject to cyber exclusion |
| Liability for breach or release of another's protected information | Typically covered for cyber perils | Covered under CGL policy, but may be subject to cyber exclusion |
| Professional liability (E&O) | Professional liability commonly excluded | Cyber exclusions commonly added to E&O policies |
| Management liability (D&O) | Management liability commonly excluded | Cyber exclusions commonly added to D&O policies |

ADJUSTINGTODAY®

## FOOTNOTES

*The concern over silent cyber was great enough to prompt a study by the Organization for Economic Cooperation and Development (OECD), a body representing countries with developed economies, entitled "Encouraging Clarity in Cyber Insurance Coverage." The report suggested that desired growth in cyber insurance is impeded by overlaps in coverage between cyber policies and property, liability, fidelity, commercial crime, and kidnap and ransom policies.

†There are some vehicle risks that "cross the line," so to speak, between auto and other property and liability exposures. These risks are mostly related to vehicles that are not required to be licensed for use on public roads, including mobile equipment, utility vehicles, and off-road, all-terrain vehicles. Policy language has been developed to address risk to these and arising from these.

‡Regarding computer hardware, as devices themselves have become smaller and more powerful, the value of hardware relative to software and data has decreased to the point where replacing hardware is of little concern in addressing cyber risk. It remains to be seen, however, how widespread integration of intelligent devices into items of tangible property will affect the hardware component of cyber losses.

§The ISO property and liability cyber exclusions are provided as "mandatory" endorsements, meaning that participating insurers are expected to add them to all applicable policies. If they don't, the insurers would be providing broader coverage than intended by ISO drafters and exceeding the parameters of the corresponding loss cost rating information. The provisions of mandatory endorsements are commonly incorporated into base policy forms when the latter undergo a general revision.

[1] Claims Mitigation Management Alliance, "The Future of the Cyber Claims Adjuster: A Jack of All Trades," CLM 2016 Cyber Liability Summit, October 5, 2016; accessed at https://www.theclm.org/Event/GeneratedScheduleAndCourses/4539

[2] Joshua Gold and Daniel Healy, "The Implications of Silent Cyber Coverage Restrictions," Risk Management, Oct. 7, 2019; accessed at https://www.rmmagazine.com/articles/article/2019/10/07/-The-Implications-of-Silent-Cyber-Coverage-Restrictions

[3] GBA Insurance, "Common Cyber Claims Insured Outside Of Cyber Policies," Oct. 23, 2023; accessed at https://www.gbainsurance.com/silent_cyber_1023

[4] GBA Insurance, "The Many Cyber Exclusions Within D&O Policies," undated; accessed at https://www.gbainsurance.com/cyber-exclusions-of-directors-insurance

### ABOUT THE AUTHOR

*Joseph S. Harrington, CPCU*

Mr. Harrington is an independent insurance writer and communications specialist. He served for over 20 years as communications director for the American Association of Insurance Services (AAIS). His work has been published in *Best's Review, Rough Notes,* publications of The Institutes, and elsewhere.

ADJUSTERS INTERNATIONAL
The *right* way to settle claims®

EMAIL
Info@AdjustersInternational.com

WEB ADDRESSES
AdjustersInternational.com
AdjustingToday.com

PUBLISHER
Gregory P. Raab, MBA

EDITOR
Ethan A. Gross, JD

***ADJUSTING TODAY®*** is published as a public service by Adjusters International, Ltd. It is provided for general information and is not intended to replace professional insurance, legal or financial advice for specific cases.

There are 23 back issues of AT at www.adjustingtoday.com.



***ADJUSTING TODAY®*** *is published by Adjusters International Ltd. to educate professionals and consumers on significant issues for first-party property insurance markets and claims. A.I. is a consortium of the nation's premiere public adjusting firms covering all 50 states, U.S. Possessions, the Caribbean, Canada, and selected international locations. Our member firms help businesses and homeowners get through some of life's greatest catastrophes, by shouldering the burden of managing property insurance claims. Adjusters International represents policyholders only. We do not represent insurance companies. Our principal mission is to support families in their property, financial and emotional recovery; and to assist businesses with their property losses, including interruption of business, retaining employees, and serving customers.*

*For help with a first party insurance claim please email info@adjustersinternational.com or visit our website at www.adjustersinternational.com.*

Follow *Adjusting Today* on Facebook & X:

Facebook.com/AdjustersInternational  X.com/AdjustingToday