



Arthur J. Gallagher & Co.

GALLAGHER CYBER LIABILITY PRACTICE

Cyber Risk Insurance Advisory & Risk  
Management Capabilities



# Cyber Risk Exposures and Solutions

Arthur J. Gallagher & Co.'s Cyber Liability Practice has the expertise and the desire to deliver a full complement of cyber risk management and insurance services. As cyber risk continues to evolve, thought leadership is of the utmost importance. Our thought leaders are based in the United States and the United Kingdom. We focus on cyber risk exclusively. We are keenly aware of the evolving risk landscape and are uniquely positioned to share our knowledge, expertise and experience for the benefit of our clients.

Virtually all organizations have implemented computer networks, mobile communications and social media initiatives. As technology is integrated into all aspects of an organization's operation, an organization's risk profile is materially altered. Matters of cyber risk have become commonplace, and the reliance upon technology in business can result in an invasion of privacy, viruses, errors or omissions, intellectual property infringement, business interruption, extra expense and damage to data. Emerging issues such as bodily injury, property damage and reputational damage are now a reality. Awareness coupled with public outcry and regulation has made cyber security a top priority. Consequently, organizations are constantly seeking meaningful solutions to manage the financial costs, operational risks and other emerging exposures to cyber risk. Unfortunately, even the most vigilant network security and most comprehensive privacy policies are vulnerable.

# Cyber Risk Exposures

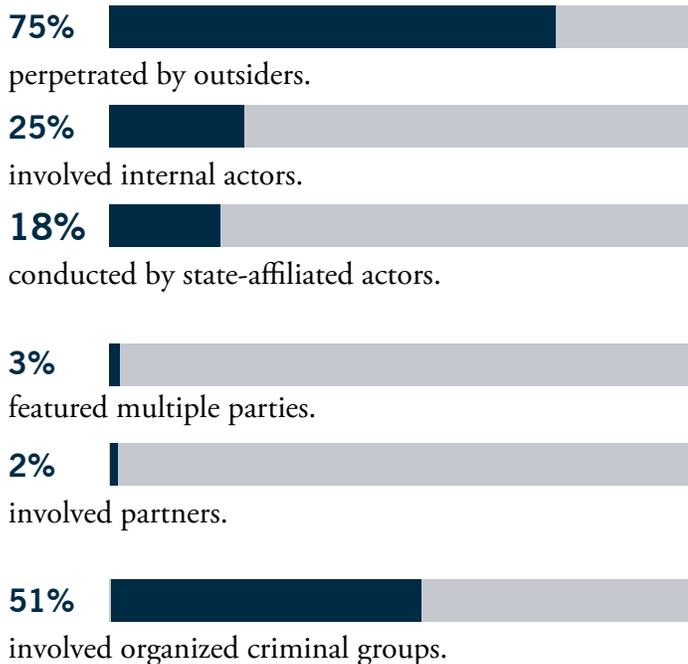
Gaining unauthorized access to computer systems and information is a direct threat to security and privacy. The most common security and privacy threats arise from:

1. Hacking—Use of a computer to gain unauthorized access to data in a system
2. Malware—Short for malicious software, malware is any software used to disrupt computer operations, gather sensitive information or gain access to private computer systems (Includes Ransomware)
3. Social Engineering—The psychological manipulation of people into performing harmful actions or divulging confidential information
4. Human Element (Errors/Mistakes/Malicious)—While these threats may lack malicious intent, the human element is uncontrollable

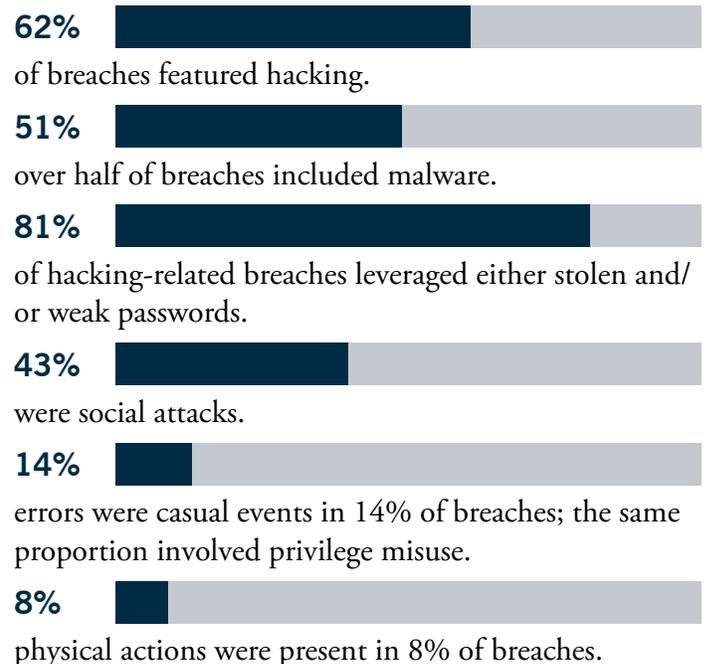
It is important to understand the core motivations behind security and privacy threats. Drivers include:

- Seeking **financial gain** by obtaining PII and selling or using it for identity theft purposes
- Seeking a **competitive advantage** by accessing confidential information such as trade secrets, formulas, designs processes and methods
- **Espionage** conducted by, or on behalf of, nation states
- “Hactivists” with an **agenda or desire to expose a perceived injustice**
- Cyber-terrorists motivated by **social, ideological, religious or political objectives**
- Thrill seekers with no agenda other than **the challenge of hacking**

## Who’s behind the breaches?



## What tactics do they use?



Source: Verizon’s 2017 Data Breach Investigations Report - Executive Summary

## Traditional Cyber Insurance Protection

Surprisingly, cyber insurance is now starting to mature as an insurance product. Many known cyber risks have been identified, quantified and are part of a “traditional” cyber insurance policy. “Traditional” cyber insurance was developed to address *known gaps* in coverage that are not covered in other insurance policies. “Traditional” cyber insurance coverage, which is widely available, is characterized by the following robust insuring agreements (Summary of terms not intended to be all encompassing—please reference insurance-specific policy forms and endorsements for exact language).

## Available Traditional Cyber Insurance Solutions

### THIRD-PARTY LIABILITY

*Organization is being held liable as a result of a lawsuit or demand for money or injunctive relief*

#### Network Security Liability

Provides liability coverage if an insured's computer system fails to prevent a Security Breach or a Privacy Breach

#### Privacy Liability

Provides liability coverage if an insured fails to protect confidential electronic or non-electronic information in their care custody and control

#### Regulatory Liability

Coverage for lawsuits or investigations by Federal, State, or Foreign regulators relating to Privacy Laws (includes fines and penalties where insurable by law)

#### PCI DSS Assessments

Coverage for contractual assessments, fines and penalties owed under the terms of a Merchant Services Agreement due to non-compliance with the Payment Card Industry Data Security Standard (PCI-DSS) and as the result of a data breach

#### Media Liability

Covers the insured for Intellectual Property and Personal Injury perils the result from dissemination of content (coverage for Patent and Trade Secrets are generally not provided)

### FIRST-PARTY (BREACH RESPONSE COSTS)

*No liability "to others" exists, but Organization needs to respond to mitigate liability under privacy regulations or from third parties*

<b>Crisis Management/ Breach Response</b>	Legal Expenses	First-party legal expenses to review and determine responsibilities under Privacy Breach Law
	Forensic Investigations	First-party expenses to investigate a system intrusion into an insured computer system
	Credit Monitoring Expense	First-party expenses to provide up to 12 months credit monitoring
	Notification Expense	First-party expenses to comply with Privacy Law notification requirements
	Public Relations	First-party expenses to hire a Public Relations firm

### FIRST-PARTY (OPERATIONAL COSTS)

*Operational impact on an organization computer system – forensics services, other extra expense or lost income*

<b>Cyber Extortion</b>	Payments made to a party as a result of a threat to breach or an actual breach of an insured's computer system in order to avert a cyber-attack or regain access to a computer system as a result of a cyber-attack; includes payments for approved services such as computer forensics investigations
<b>Data Recovery</b>	First-Party expenses to recover data damaged on an insured computer system as a result of a failure of security
<b>Business Interruption</b>	First-Party loss for lost income from an interruption to an insured computer system as a result of a failure of security or system failure

# Cyber Insurance Distribution

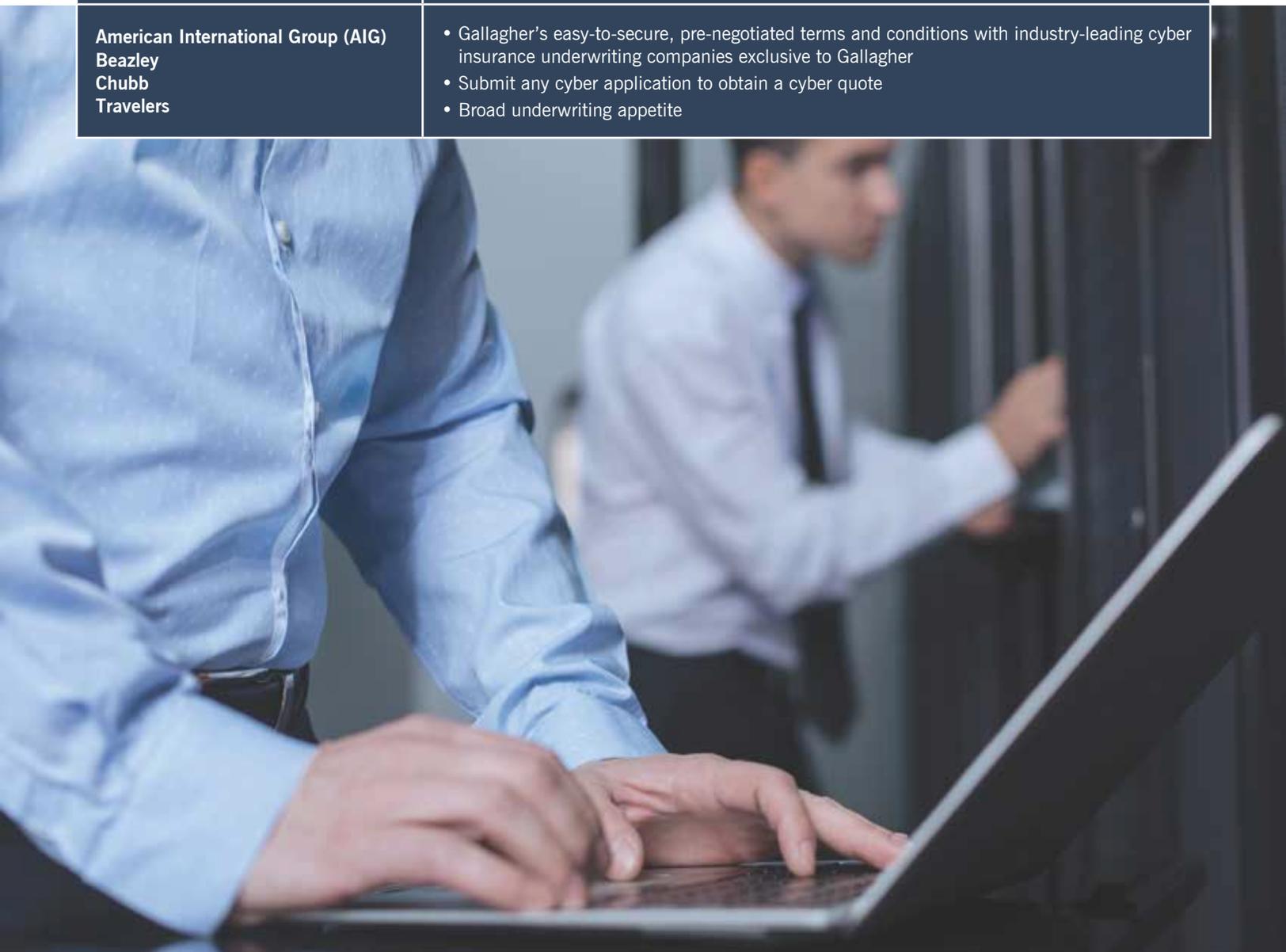
## Open Market Brokerage: Meeting the Needs of All Clients

Our Cyber Liability Practice represents a diverse cyber insurance marketplace. We have access to over 50 markets offering specific cyber insurance coverage. Through our relationships we have developed manuscripted language and/or pre-negotiated endorsements with many of our major cyber insurance carriers to meet the unique needs of our clients.

## Streamlined Solutions

Cyber Insurance Placements for Small and Emerging Businesses  
(up to \$250M in annual revenue/operating budget)

STREAMLINED SOLUTION	DESCRIPTION OF CYBER SOLUTION
<b>AJGCyber.com</b> (Underwriters at Lloyd's, London)	<ul style="list-style-type: none"><li>• A Gallagher proprietary online cyber distribution platform that provides market-leading policy wording.</li><li>• Online application process</li><li>• Answer 4–6 online questions to receive a bindable quotation</li><li>• Very few excluded classes</li></ul>
<b>American International Group (AIG)</b> <b>Beazley</b> <b>Chubb</b> <b>Travelers</b>	<ul style="list-style-type: none"><li>• Gallagher's easy-to-secure, pre-negotiated terms and conditions with industry-leading cyber insurance underwriting companies exclusive to Gallagher</li><li>• Submit any cyber application to obtain a cyber quote</li><li>• Broad underwriting appetite</li></ul>



# Cyber Risk Management Solutions

As cyber threats continue to exploit organizations, cyber security has become a top five management concern, oftentimes ranking first or second in priority. Organizations are constantly seeking solutions to manage their evolving vulnerabilities to cyber risk. Clients need thought leaders in the cyber space. Gallagher's Cyber Liability Practice is dedicated to an analytical philosophy, which involves comprehensive risk management cyber services. Our robust risk management services platform includes:

- Best practices (policies, articles, white papers and webinars)
- Proprietary benchmarking/Third-party benchmarking
- Network assessments
- Cost of a breach calculator
- Coverage gap analysis
- Contract analysis
- Incident response planning (spells out steps to be taken in event of a breach—including breach coach)
- Insurance policy design and implementation
- Complimentary Preventive Services
- Strategic Vendor Relationships



## Evaluating Emerging Cyber Insurance Concerns

It has become clear that cyber insurance is evolving once again. As the consequences of a cyber event become ever more far reaching, “traditional” cyber insurance has created a foundation of protection. However, this foundation must be used as a starting point to identify and evaluate “emerging” cyber risks. Emerging cyber risks may result in physical harm and other financial/non-financial consequences. Many of these emerging cyber risks are currently uninsured because they have been intentionally left unaddressed by cyber insurance carriers due to unwillingness to accept the risk, are overlooked by cyber insurance carriers, or simply are not yet known risks that can be insured.

Therefore, it is essential to recognize the depth of coverage that a traditional cyber insurance policy affords. Understanding where traditional cyber insurance policies and other P&C insurance policies complement, overlap or exclude a cyber exposure is critical. Traditional cyber insurance policies may not provide coverage for cybersecurity breaches resulting in bodily injury, property damage, theft of funds, and reputational damage, amongst others.

## Analysis of Gaps & Overlaps

A prudent exercise to accomplish an understanding of cyber risks that are insured or uninsured is to perform a thorough cyber insurance gap analysis. As part of this process, evaluation and isolation of valuable “at risk” assets should be analyzed and discussed to determine how current insurance risk transfer products would provide recovery in the event of a cyber event. In some cases, uninsured issues will become evident and emerging areas of concern will need to be discussed.

## Cyber Liability Practice—Education

Gallagher’s Cyber Liability Practice is dedicated to continued education through the following:

- Knowledge center ([www.ajg.com/cyber](http://www.ajg.com/cyber))
- CyberUniversity webinars
- Experts directory (access to qualified third-party providers of breach-related services)
- Gallagher cyber news updates
- Cyber market reports
- Third-party cyber benchmark reports and updates

## KNOW THE FACTS



43%

of cyber-attacks targeted small and medium-sized businesses<sup>1</sup>



22%

of companies had a loss of customers<sup>4</sup> as a result of a breach



66%

of respondents say their technologies currently in use can't detect and block most cyber-attacks<sup>2</sup>



60%

of small businesses breached are out of business within 6 months<sup>3</sup>



\$879,582

total average cost of a data breach involving theft of IT assets<sup>2</sup>

1. Source: Symantec

2. Source: The 2016 State of SMB Cybersecurity — Ponemon Institute and Keeper Security

3. Source: National Cyber Security Alliance

4. Source: Cisco 2017 Security Capabilities Benchmark Study, [www.cisco.com/go/acr2017](http://www.cisco.com/go/acr2017)

# Cyber Claim Advocacy

We combine our extensive knowledge of cyber liability with our experience as claim advocates to achieve positive claim results. We have a deep understanding of the cyber liability claim lifecycle, which begins at the time of a breach event. We emphasize breach preparedness at the strategic planning phase when procuring insurance coverage. Choosing the appropriate vendor relationships either through a pre-approval process or an insurance carrier panel is essential to a successful breach response. In addition, a proper breach response can better position any litigation defense.

It is important to understand your obligations and duties in the event of a breach situation. We have prepared the following important guidelines to assist you when a breach results:

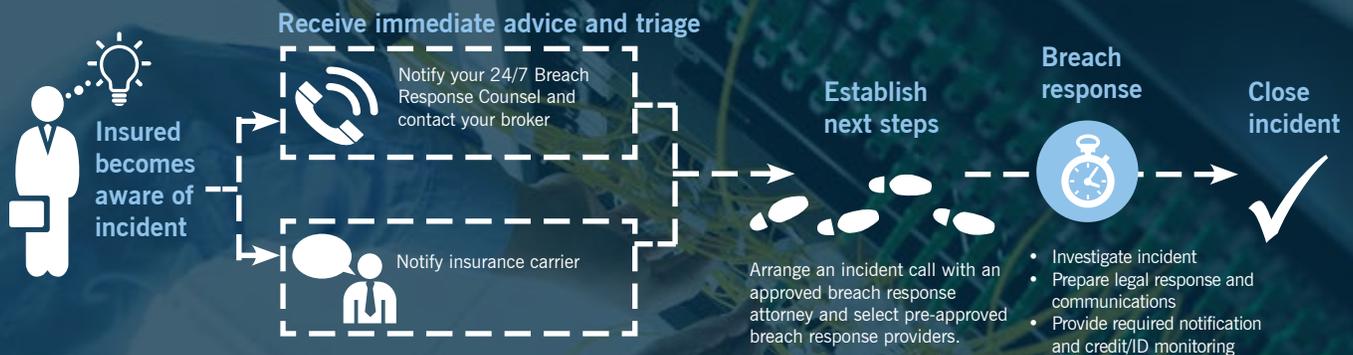
Be sure to follow the requirements of the cyber insurance policy conditions relating to prior approval and utilization of panel service providers. Additionally:

1. Educate and regularly train staff on internally reporting potential or actual breaches or suspicious activity. Identify key internal staff responsible for receiving such reports and notifying appropriate internal and external parties.
2. Select a qualified breach response attorney. Interview several firms and choose 2–3 qualified firms in order of preference in the event a conflict exists. Many cyber insurance policies designate 3–4 qualified and preapproved breach response attorneys. Some policies allow the insured to select counsel of their choice.

The following service providers should be engaged at the time of a breach through your selected law firm to protect the attorney/client privilege:

1. Select a forensic investigator. Interview several firms and choose 2–3 qualified firms in order of priority should a conflict exist. If your business processes credit card information, also identify 2–3 Payment Card Industry Forensics Investigators (PFIs) in case such an investigation is needed.
2. Select a qualified breach notification service provider (including printing and mailing notices and call center).
3. Select a qualified credit monitoring/ID monitoring service provider.
4. Select a qualified public relations firm.
5. Select a qualified defense attorney for post-breach defense litigation.

## Duties in the event of a breach or extortion demand



## Cyber Insurance Coverage

### Initial Coverage Evaluation

1. Expect to receive an initial acknowledgement of the claim from the cyber insurance company
2. Generally, within 30 days, a formal claim evaluation will be provided by the insurance company determining if coverage for the breach is available
3. The insurance company will likely follow up for additional information about the breach
4. The insurance company will provide confirmation of the approved service providers (if any) and the scope of services.



## Breach Response Notification Requirements

At the time of a breach, the following steps should be taken to properly position your organization to respond to a breach and to ensure that insurance will apply:

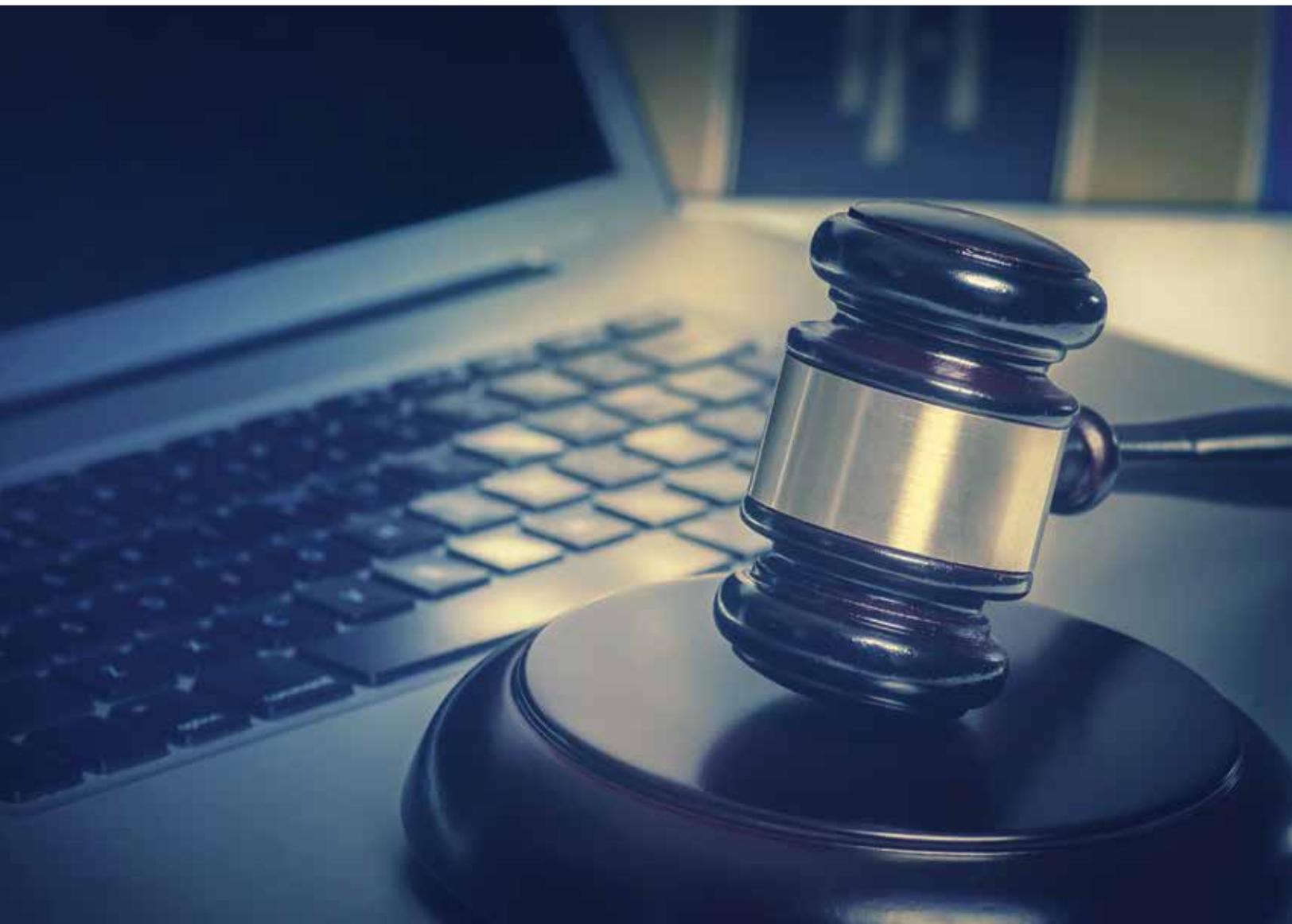
1. Contact your qualified breach response attorney immediately to establish attorney/client privilege and to begin the process of investigating the incident. The breach response attorney will also work with you to ensure all potentially relevant information and documentation is preserved and protected from destruction.
2. Retain a forensics investigator with the guidance of the breach response attorney. The breach response attorney will engage the forensic investigator on behalf of your company to protect the exchange of information under attorney/client privilege.
3. The choice of counsel and forensics investigator may need to be approved by your insurance company. Immediate notification to the insurance company, based upon the specific conditions of the cyber insurance policy may be required. Also, notify your insurance broker. The notice should include all facts (but only facts) available at the time of the notice. Many insurance companies have a 24-hour cyber breach hotline that will allow for immediate direct interaction with the insurance company, which is especially important if prior approval is required before engaging a breach attorney and forensics investigator. Continue to provide additional details to the insurance company and the insurance broker as they become available.
4. Your qualified breach attorney will help with breach notice requirements and forensics reports to determine the breach notice requirements.

## Duties in the Event of Litigation



## Post-Breach Litigation

1. A breach often leads to litigation brought by the parties impacted by the breach.
2. If litigation results from a breach, it is important that a comprehensive breach response plan has put your organization in a defensible position. It is imperative that measures are taken before litigation to ensure that potentially relevant information and documentation is preserved and protected from destruction.
3. Select qualified defense counsel pre-approved by your insurance company. The breach response attorney could also serve as defense counsel with carrier approval. Interview several firms and choose 2–3 qualified firms in order of priority should conflict exist.



## Cyber Insurance Expertise and Experience

Arthur J. Gallagher & Co. is committed to helping our customers understand and manage the emerging exposures to cyber risk. We have allocated resources and made strategic investments in specialists with expertise in this field. We have six dedicated U.S. Cyber Directors strategically located within Gallagher to service the needs of our clients in this ever-changing cyber risk landscape. Please feel free to contact us with any questions. We look forward to working with you!

## Gallagher Cyber Liability Practice

**Adam Cottini**, Managing Director  
*Northwest & Southwest Area Director*  
adam\_cottini@ajg.com | 212.994.7048

Adam is Managing Director of the Cyber Liability Practice for Arthur J. Gallagher & Co. Adam is responsible for the overall direction of the Cyber Liability Practice, including development of state-of-the-art product solutions, insurance gap analysis, risk exposure analysis, risk modeling, benchmarking and best practices implementation. Adam has been providing cyber risk management brokerage and consulting services for over 10 years.

**Jeremy Gillespie**  
*Midwest & Great Lakes Area Director*  
jeremy\_gillespie@ajg.com | 312.803.7394

Jeremy has been brokering cyber liability products exclusively for over 7 years. He manages a robust book of cyber liability for insureds of all sizes and industries. He specializes in complex insurance policy design and risk transfer. His book of business is comprised of many high-risk classes, including higher education, retail, healthcare and public entities.

**Brendan Goodwin**  
*Northeast & Mid-Atlantic Area Director*  
brendan\_goodwin@ajg.com | 212.981.2995

Brendan is responsible for the implementation of the initiatives set forth by the National Cyber Liability Practice at the regional level. He manages a diverse book of cyber liability with clients of all sizes and industry classes. Brendan's experience with professional lines products spans cyber liability, directors & officers liability, employment practices liability, fiduciary liability and errors & omissions liability as both an underwriter and broker for more than 10 years.

**Jennifer G. Bolling**  
*Southeast & Mid-South Area Director*  
jennifer\_bolling@ajg.com | 205.986.7711

Jennifer specializes in consulting and broking services in the areas of management and professional liability insurance. Her areas of concentration focus on cyber liability, directors & officers liability, employment practices liability, fiduciary liability and errors & omissions liability. Jennifer has over 10 years of experience in professional lines brokerage placements.

**Thomas Douglass**  
*South Central Area Director*  
thomas\_douglass@ajg.com | 314.800.2225

Thomas has been focusing on risk management consultation and insurance placements of cyber, privacy, network security and technology and errors & omissions insurance products for over 10 years. In addition, he has a strong financial institution background that included cyber gap exposure analysis of financial institution products. Thomas is a frequent speaker on network security/privacy topics for local chapters of RIMS and the CPCU Society.

**Jonathan Henley**  
*South Central Area Director*  
jonathan\_henley@ajg.com | 713.800.5968

Jonathan is a licensed attorney and has 13 years of brokerage experience, including professional lines insurance. Jonathan's legal background allows him to take a unique perspective on cyber risk exposure. Prior to joining Gallagher, he practiced commercial litigation with a large Houston law firm.



Arthur J. Gallagher & Co.

### Adam Cottini

Managing Director  
Cyber Liability Practice  
212.994.7048  
adam\_cottini@ajg.com

[www.ajg.com/cyber](http://www.ajg.com/cyber)

Gallagher Cyber Liability Practice

Insurance brokerage and services to be provided by Arthur J. Gallagher Risk Management Services, Inc. and/or its affiliate Arthur J. Gallagher & Co. Insurance Brokers of California, Inc. (License No. 0D69293 and/or 0726293).

© 2017 Arthur J. Gallagher & Co. All rights reserved.

CR12GGB0717