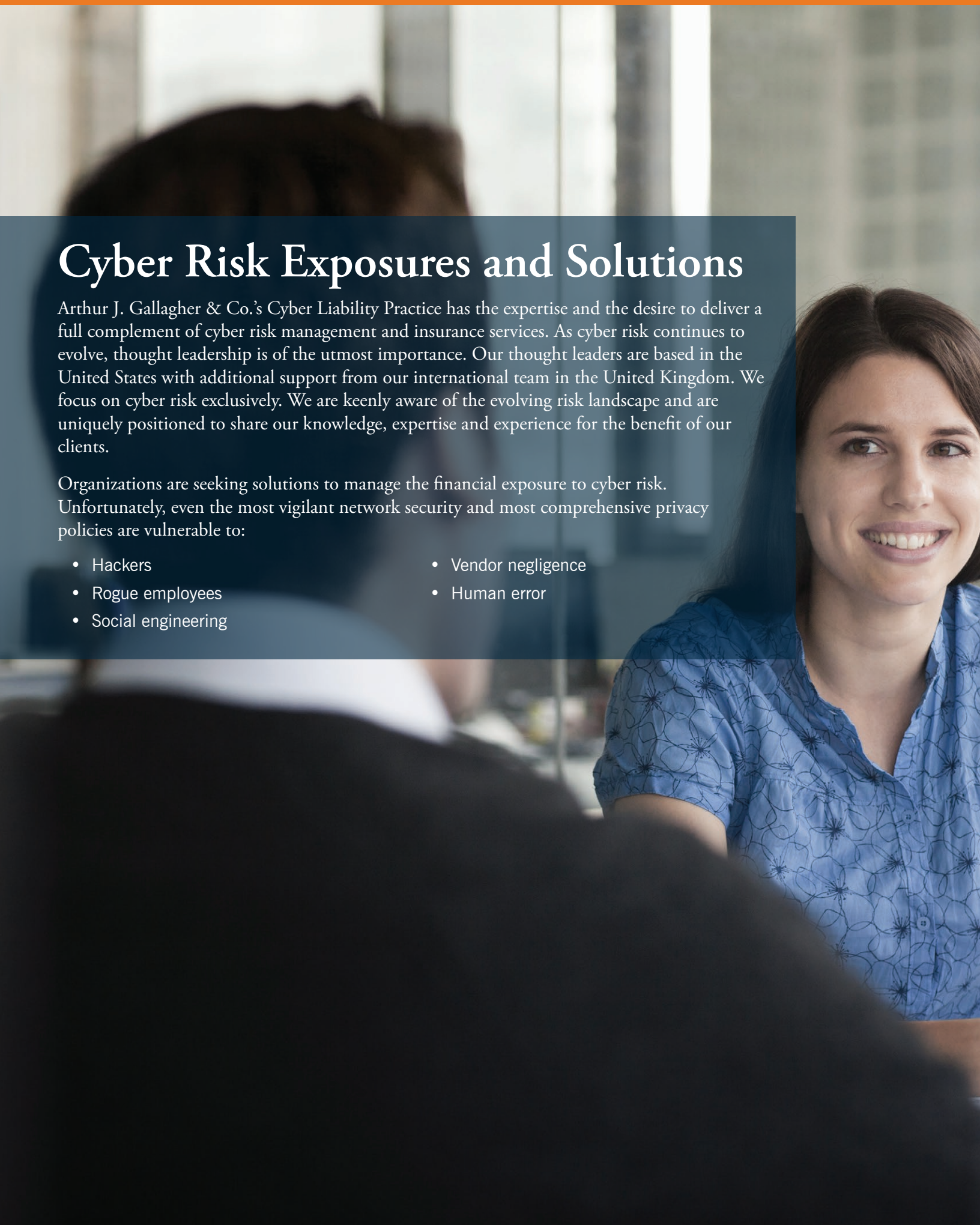
Arthur J. Gallagher & Co.

GALLAGHER CYBER LIABILITY PRACTICE

Cyber Risk Exposures and Solutions



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 with additional support from our international team in 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.

Organizations are seeking solutions to manage the financial exposure to cyber risk. Unfortunately, even the most vigilant network security and most comprehensive privacy policies are vulnerable to:

- Hackers
- Rogue employees
- Social engineering
- Vendor negligence
- Human error

Cyber Risk Exposures

The Cyber Risk Landscape

Target Corporation's data breach was disclosed in November 2013 and it marked the beginning of what was a cyber newsworthy 2014 and 2015. The well-publicized cyber breaches at Home Depot, JP Morgan Chase, Michael's Stores, the US Postal Service, Sony Pictures and Anthem were only some of the hundreds of breaches of cyber security to make headlines that have changed how all organizations view cyber risk.

Protecting Personally Identifiable Information (PII) is extremely challenging in an environment of technological advancements, rapid adoption rate of technology by consumers and the desire by users for more convenience. 2014 and 2015 have changed how organizations, consumers and regulators view cyber risk. The "it can't happen here" attitude has been replaced with the more realistic, "when will it happen to us." The exposure didn't change, rather the frequency and severity of breaches that have made the public more aware of the possibility, even the probability, of security breaches.

This awareness has made cyber security a top priority. With this priority comes the knowledge of ramifications: costly breach expenses, potential litigation, operational disruptions and reputational damage. The biggest organizations with world-class security have proven vulnerable. Proactive risk management is crucial.

Regulators are making it clear that enforcement will continue, including:

- Scrutiny under the Health Insurance Portability and Accountability Act (HIPAA) and the U.S. Securities and Exchange Commission (SEC) have become more active in reviewing disclosures of material cyber risk for publicly traded companies.
- Amendments to state laws in California and Florida
  - » Changes to how these states define personally identifiable information (user names and email addresses, in combination with passwords and security questions).
- Desire of New York State's Attorney General to make similar amendments to New York's privacy law.
- A federal data breach law has been under review for several years.
  - » Federal cyber regulations are expected to come back on a national level with changes in congressional power.

Rationale for Insurance

The growth of electronic networks and the increased volume of data has substantially changed the risk profile of virtually all organizations. Utilization of cloud computing, mobile communications and social media continue to complicate the cyber risk landscape. The size and scope of the liability is starting to become clearer as we begin to accumulate data on major cyber events. Generally, traditional insurance policies are not responsive to the types of financial loss claims as a result of a security breach. We have seen part of the Target breach litigation settle for over $30 million and the highly publicized expenses associated with Anthem exceed $100 million in breach response costs alone.

Available Insurance Solutions

EXPOSURE CATEGORY		DESCRIPTION
Network Security Liability		Provides liability coverage if an insured's computer system fails to prevent a security 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.
PCI Assessments		Coverage for contractual assessments, fines and penalties owed under the terms of a Merchant Services Agreement due to noncompliance with the Payment Card Industry Data Security Standard (PCI-DSS) and as the result of a data breach.
Breach Response	Legal Expenses	First-party legal expenses to review and determine responsibilities under Privacy Breach Law.
	Notification Expense	First-party expenses to comply with privacy law notification requirements.
	Credit /ID Monitoring	First-party expenses to provide up to 12 months credit monitoring.
	Forensic Investigations	First-party expenses to investigate a system intrusion into an insured computer system.
	Public Relations	First-party expenses to hire a public relations firm.
Media Liability		Covers the insured for intellectual property and personal injury perils that result from content.
Cyber Extortion		Payments made to a party threatening to attack an insured's computer system in order to avert a cyber attack.
Data Recovery		First-party expenses to recover data damaged on an insured computer system as a result of a failure of security.
Business Interruption		First-party expenses for lost income from an interruption to an insured computer system as a result of a failure of security.
Errors & Omissions (E&O)		Technology E&O/Miscellaneous E&O coverage for wrongful acts committed by or on behalf of the insured.

Open Market Brokerage

(Solutions for all clients of all sizes)

Our Cyber Liability Practice represents a diverse cyber insurance marketplace. We have access to over 40 markets offering cyber liability coverage. Through our relationships we have developed manuscripted language and/or endorsements with many of the major cyber insurance carriers to meet the unique needs our clients. Our cyber experts work with the following insurance carriers on a daily basis:

- ACE
- AIG
- Allied World
- Argo
- Arch
- Axis
- BCS Insurance Company
- Chubb
- CNA
- CV Starr
- Endurance
- Freedom Specialty
- Hartford
- HCC
- Ironshore
- Liberty
- Lloyd's (Beazley, Brit, Barbican, Hiscox, Kiln and more)
- Markel
- Philadelphia
- Swiss RE
- Travelers
- XL
- Zurich

Risk Management Solutions

(Specialty solutions specifically designed to meet the needs of clients with Annual Sales/Budget greater than $100 million)

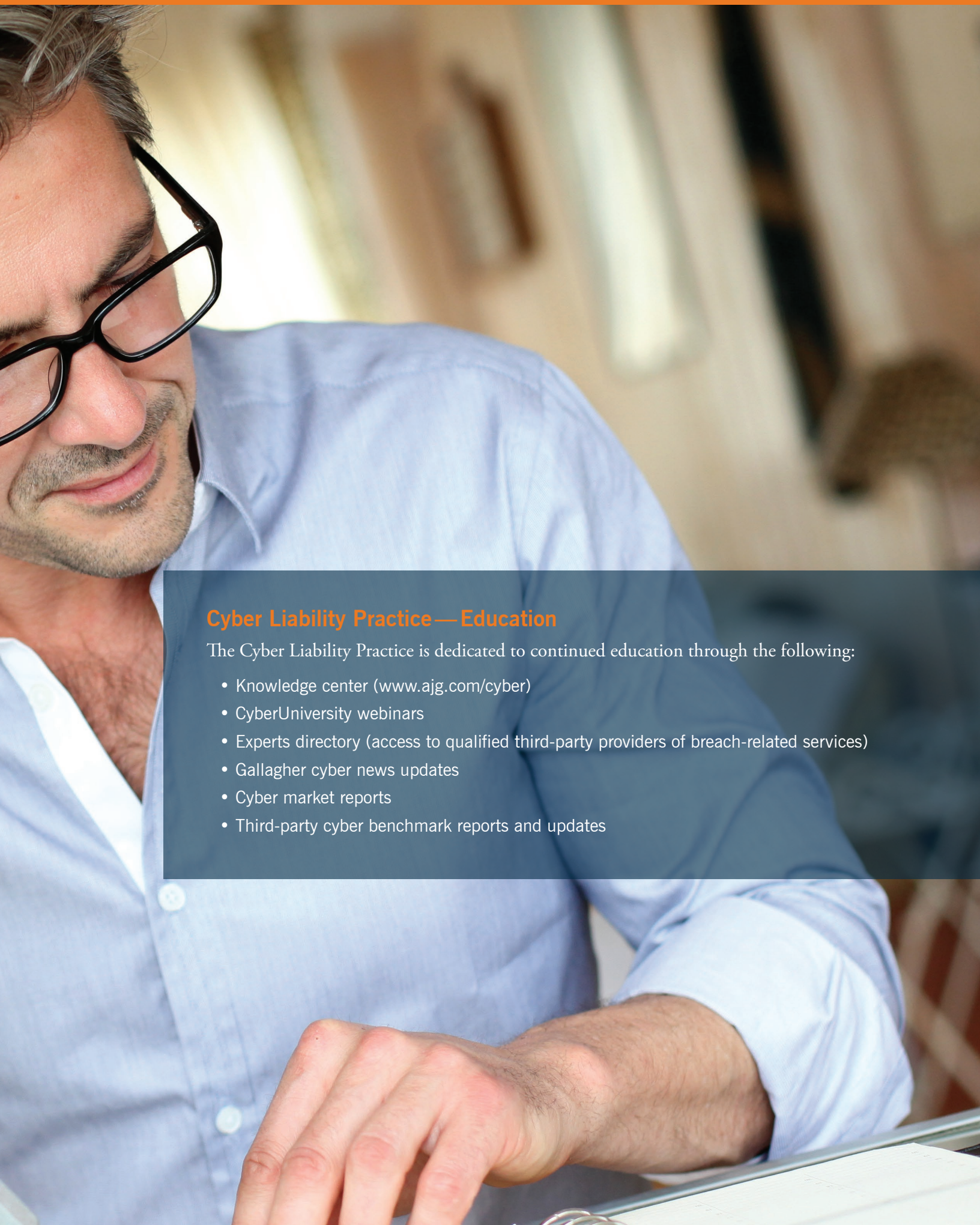
Clients with annual sales/budgets exceeding $100 million and in particular high risk classes, (i.e., healthcare, higher education, government, retail, financial institutions and technology) need thought leaders in the cyber space. Gallagher's Cyber Liability Practice is dedicated to an analytical philosophy, which involves comprehensive risk management cyber services. Our robust risk management services platform includes:

- Incident response planning (spells out the steps to take in the event of a breach—including Breach Coach)
- Best practices (polices, articles, white papers and webinars)
- Proprietary benchmarking/Third-party benchmarking
- Quick audit—network assessments
- Cost of a breach calculator
- Coverage gap analysis
- Policy design and best-in-class terms
- Contract analysis
- Vendor management
- Insurance policy design and implementation
  - » We can secure cyber insurance through an open brokerage approach using our pre-negotiated terms as well as through our proprietary insurance policy form.
  - » Our proprietary policy form is best-in-class manuscript language supported through our Gallagher UK team.

Small & Middle Market Client Solutions

(Clients with less than $100M in Annual Sales/Budget)

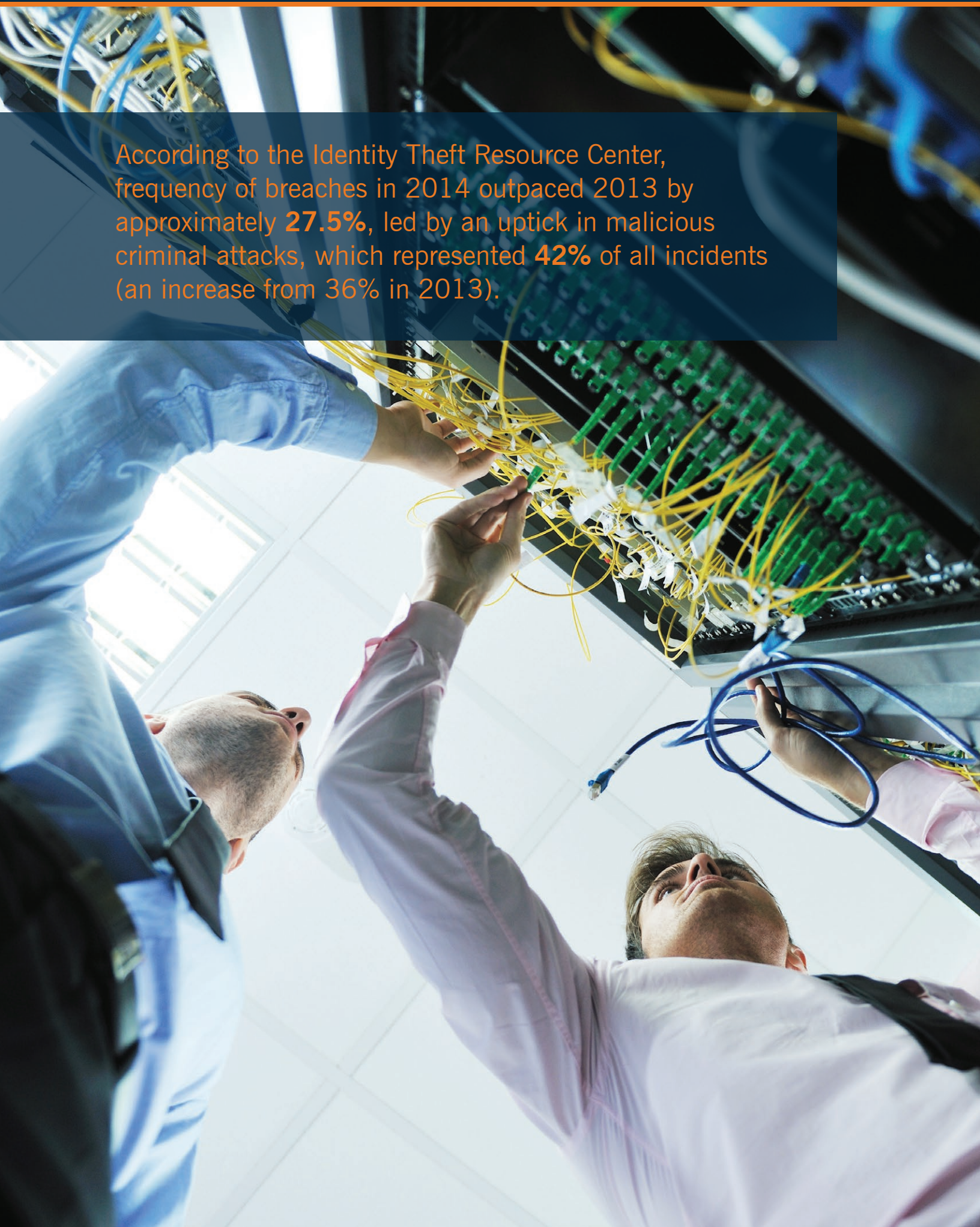
AJGcyber.com AJGcyber.com provides best-in-class policy wording supported by Lloyd's of London.	• Online application • Answer 4–6 online questions to receive a bindable quotation • Very few excluded classes
AJGcyber@beazley.com Beazley is known as a premier underwriter of cyber liability, and together we have partnered with Beazley to make it easy for you to receive a Beazley Cyber quote.	• Pre-negotiated Gallagher Amendatory • Receive Beazley's well-known cyber policy with even broader terms that have been completely vetted by Gallagher's Cyber Liability Practice • Submit any cyber application to obtain a Beazley cyber quote
Pre-Negotiated Endorsements with Select Cyber Markets	• We can secure cyber insurance from many of the major cyber carriers with pre-negotiated Gallagher terms (Including Ace, AIG, Chubb and Travelers) • Submit any cyber application to obtain a cyber quote
Open Brokerage	• We can access additional cyber carriers to obtain alternate options when necessary



Cyber Liability Practice — Education

The Cyber Liability Practice is dedicated to continued education through the following:

- Knowledge center (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



According to the Identity Theft Resource Center, frequency of breaches in 2014 outpaced 2013 by approximately **27.5%**, led by an uptick in malicious criminal attacks, which represented **42%** of all incidents (an increase from 36% in 2013).

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 pre-approved breach response attorneys. Some policies allow the insured to select counsel of their choice.

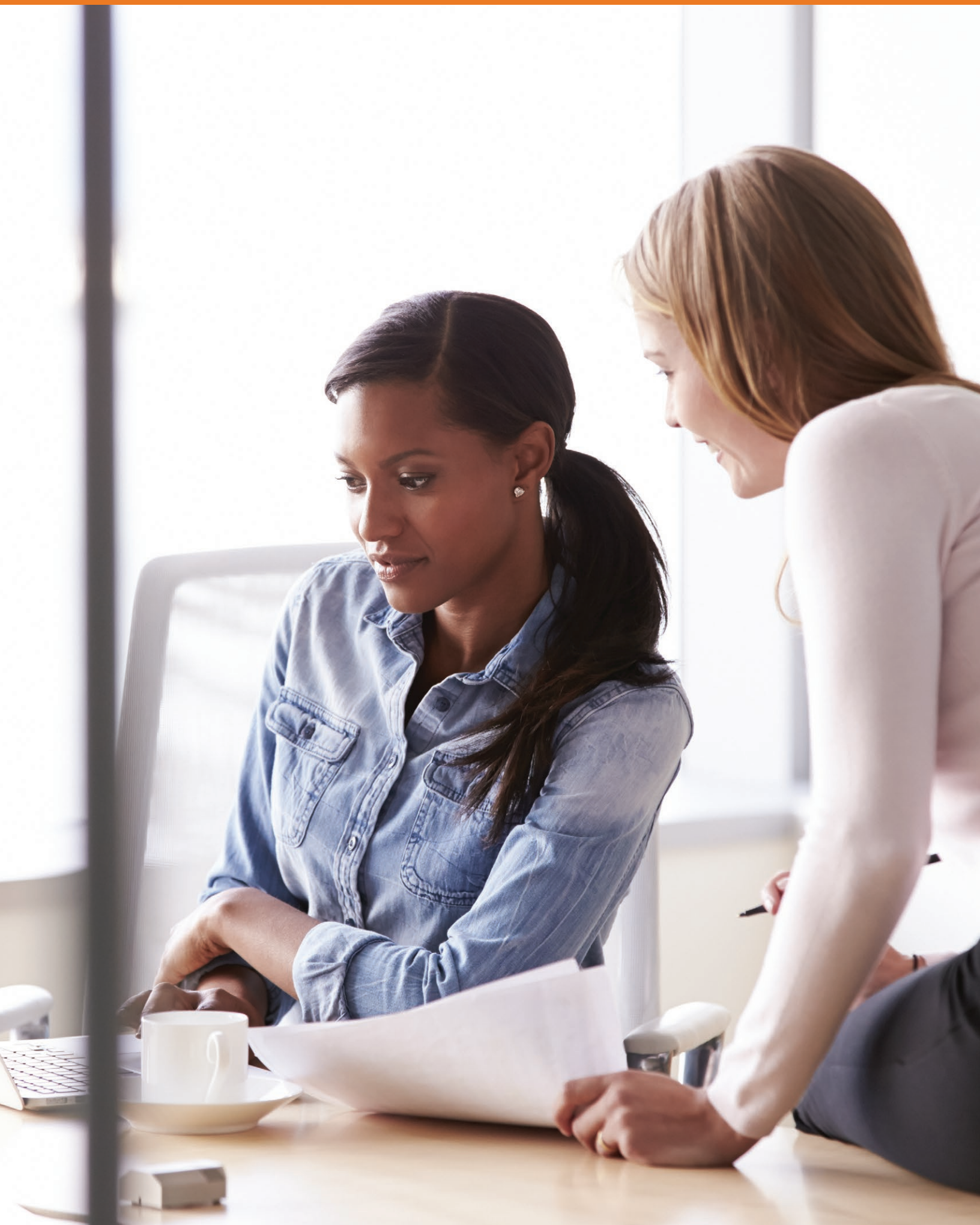
The following service providers should be engaged at the time of a breach through your selected law firm to protect the attorney/client privilege:

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.

B. 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.



C. 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.

D. 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 Liability 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 five dedicated 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!

MANAGING DIRECTOR

NORTHEAST & WEST REGIONAL DIRECTOR

Adam Cottini *(New York, NY)*

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.

Contact: 212.994.7048 | Adam_Cottini@ajg.com

MIDWEST & WEST REGIONAL DIRECTOR

Jeremy Gillespie *(Chicago, IL)*

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 entitles.

Contact: 312.803.7394 | Jeremy_Gillespie@ajg.com

SOUTHEAST REGIONAL DIRECTOR

Jennifer G. Bolling *(Birmingham, AL)*

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.

Contact: 205.986.7711 | Jennifer_Bolling@ajg.com

CENTRAL REGIONAL DIRECTOR

Thomas Douglass *(St. Louis, MO)*

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.

Contact: 314.800.2225 | Thomas_Douglass@ajg.com

SOUTH CENTRAL REGIONAL DIRECTOR

Jonathan Henley *(Houston, TX)*

Jonathan is a licensed attorney and has 12 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.

Contact: 713.800.5968 | Jonathan_Henley@ajg.com

Arthur J. Gallagher & Co.

Reduce your risk. Contact us today.

Brendan Goodwin
Regional Director
Cyber Liability Practice
212.981.2995

Brendan_Goodwin@ajg.com

Adam Cottini
Area Senior Vice President
Managing Director, Cyber Liability Practice
212.994.7048

Adam_Cottini@ajg.com

www.ajg.com/cyber

15BSD28737B