



Arthur J. Gallagher & Co.

GALLAGHER CYBER LIABILITY PRACTICE



Tailored Solutions for Cyber Liability and Professional Liability



Are you exposed to cyber risk?

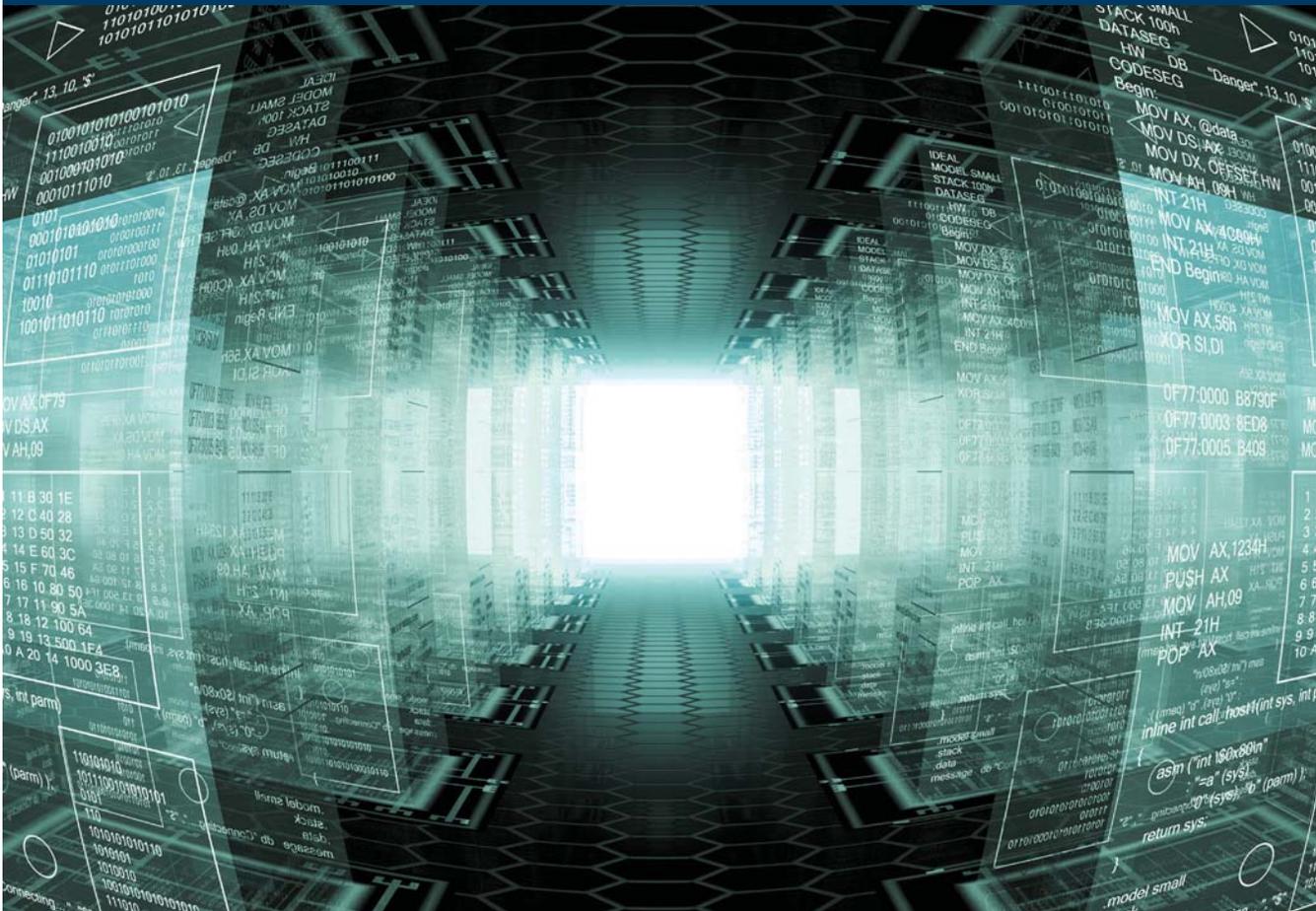
Like nearly every other business, you have probably capitalized on the advancements in technology today through the digitization of your company's important information. Whether it's your customer records, employee information, patient information or student records, all are digitized and transferable through email or accessible on your network.

This convenience comes with substantial cyber risk to your company and the clients you serve. Network security and privacy losses related to viruses, hacking, digital defamation and intellectual property infringement are becoming commonplace. Unfortunately, it's unlikely that these new risks are covered by your existing insurance policies.

Gallagher's Cyber Liability Practice is a dedicated team of recognized leaders providing information risk management services and risk transfer products. We broker information security services and insurance products for the digital world.

Gallagher's Cyber Liability Practice expertise includes:

- Analysis of current cyber risk coverage gaps
- Identifying potential future gaps in coverage based on trends and expectations of carriers
- Matching exposures to these potential gaps
- Designing risk management solutions



The most vigilant network security and most comprehensive privacy policies remain vulnerable to hackers, rogue employees, social engineering and human error.

A checklist for assessing your level of cyber risk.

These questions can give you a quick look into many of the areas of vulnerability that companies overlook.

Are you aware of the coverages and gaps within standard property & casualty policies with respect to network security and privacy events?	<input type="checkbox"/> YES <input type="checkbox"/> NO
Have you budgeted for a cyber security or privacy event?	<input type="checkbox"/> YES <input type="checkbox"/> NO
Have you assessed your exposure to privacy regulation? Lawsuits by your customers?	<input type="checkbox"/> YES <input type="checkbox"/> NO
Do you understand what regulated data you have, where it exists and in what format?	<input type="checkbox"/> YES <input type="checkbox"/> NO
Do you have an incident response plan and/or a business continuity plan?	<input type="checkbox"/> YES <input type="checkbox"/> NO
Are there processes and procedures in place regarding data retention and data destruction?	<input type="checkbox"/> YES <input type="checkbox"/> NO
Do you track and monitor compliance on an ongoing basis?	<input type="checkbox"/> YES <input type="checkbox"/> NO
Are all of your procedures and policies with respect to your regulatory obligations documented?	<input type="checkbox"/> YES <input type="checkbox"/> NO
Does your organization have processes to review and update privacy policies and disclaimers to customers?	<input type="checkbox"/> YES <input type="checkbox"/> NO
Have you assessed how vulnerable you are to attack on the confidentiality, integrity and availability of your data and systems?	<input type="checkbox"/> YES <input type="checkbox"/> NO
Is your risk exposure to technology or operations failures at your vendors and service providers fully documented?	<input type="checkbox"/> YES <input type="checkbox"/> NO
Have you protected your company in contracts with vendors?	<input type="checkbox"/> YES <input type="checkbox"/> NO
Have you fully assessed the physical security controls at each of your sites (data center, home office, field offices and other sites)?	<input type="checkbox"/> YES <input type="checkbox"/> NO

“CYBER LIABILITY IS ONE OF THE LARGEST AND MOST NEGLECTED AREAS OF RISK THAT COMPANIES FACE TODAY. TECHNOLOGY PROVIDES GREAT LEVERAGE IN TODAY’S GLOBAL ECONOMY, BUT IT ALSO INTRODUCES NEW AND INCREASING CHALLENGES TO A BUSINESS LEADER. FROM HACKERS TO DISGRUNTLED EMPLOYEES, MOST COMPANIES ARE RELATIVELY UNPREPARED FOR THE DAMAGE THEY COULD EXPERIENCE.”

– Mark Greisiger, NetDiligence



Why cyber insurance?

- Frequency of privacy breaches are on the rise.
- Threats and vulnerabilities are getting dramatically worse.
- More than 47 states, including U.S. territories, have enacted privacy laws in response to the increased frequency of privacy breaches.
- International privacy regulations are drastically increasing at a noticeable rate.
- Corporate governance requires that organizations address information technology risks.
- Shareholders expect that their investment is protected from adverse market fluctuations.
- Publicly traded companies and large privately held corporations could experience shareholder litigation due to mismanagement of cyber risk.
- The plaintiffs’ bar is becoming more active in pursuing class-action litigation.
- Contracts may require cyber liability insurance.
- Cyber liability insurance can mitigate the financial impact on a company.

What is the financial impact of a security/privacy breach?

No industry is immune to a data breach whether intentional or unintentional, electronic or nonelectronic. The costs to remedy and respond to such breaches are significant as noted below.

- Cost to defend and/or settle litigation from customers or employees for identity theft.
- Cost to defend and/or settle litigation from banks to recover the value of reissuing credit cards or fraudulent transactions.
- Cost to defend and/or settle regulatory investigations.
- Cost to respond to regulatory laws.
- Cost to defend and/or settle unauthorized access or unauthorized use.
- Cost to defend and/or settle allegations that malicious code (such as viruses) caused harm to the data or computer systems of third parties.
- Cost to defend and/or settle allegations that an insured's computer system denied a third party the ability to conduct transactions.
- Cost to defend and/or settle litigation from customers or employees for identity theft.
- Cost to investigate and determine the cause of a security or privacy breach, including computer forensics.
- Cost to hire a public relations or crisis management firm to mitigate against reputational harm.
- Cost for legal counsel related to privacy and notification laws.

What could a cyber breach cost you?*

\$154 Globally

Average cost per record.

\$217 U.S.

Average cost per record
(includes response costs,
defense and damages).

\$3.79M

Average total cost per breach.

*2015 Annual Study: Cost of Data Breach Study: Global Analysis; The Ponemon Institute, LLC

A range of coverages that you should explore.

Network Security Liability

Provides liability coverage for damages and claim expenses arising out of an actual or alleged act, error or omission resulting in:

- The failure to prevent unauthorized access/use to system that results in:
 - The destruction, deletion or corruption of electronic data;
 - Theft or loss of data; or
 - Denial of service attacks against internet sites or computers.
- The inability of a third party, who is authorized to do so, to gain access to your system.
- The failure to prevent transmission of Malicious Code from your system to third-party computers and systems.

Privacy Liability

Provides liability coverage if an insured fails to protect electronic or nonelectronic private or confidential information in their care custody and control.

Privacy Regulatory Proceeding

Provides coverage for defense expenses, and in some cases penalties/fines, incurred from a regulatory proceeding resulting from a violation of a privacy law caused by a covered security breach.

Breach Response Expenses

Covers crisis management, including credit monitoring services and public relations expenses incurred resulting from a security or privacy breach. Also pays costs of notifying consumers as required by various state, federal or international laws or regulations.

Real-World Examples of Cyber Claims

Security Liability: A hacker infiltrated an online shopping website and stole 300,000 customer credit card numbers. The website faced claims from the customers for unauthorized charges made on the credit cards.

Security Liability: A disgruntled employee corrupted data in the company's system that was used to upgrade a product already on the market. The corruption caused damage to clients trying to upgrade the product as well as delays, cost overruns, etc., resulting in a loss of \$50 million.

Privacy Liability: A bank employee obtained unauthorized access to the computer system in order to search for potential clients for a friend in the real estate business. The employee provided confidential information regarding consumers to the friend. The scheme was discovered after the confidential information was leaked to another party and subsequently used as a part of an identity theft scheme.

Privacy Liability: A business owner was sued after identity thieves were able to obtain personal consumer information of customers from a dumpster of discarded files.

Privacy Regulatory: Several hospital patient records were compromised when a hacker infiltrated the hospital's network. The Office for Civil Rights (OCR) contacted the hospital for further details of the security breach and found the hospital was not in compliance with HIPAA regulations. The hospital was fined for noncompliance.

Real-World Examples of Cyber Claims (cont.)

Breach Response: A national retail chain estimates that the costs from one of the largest computer data breaches in corporate history, in which more than 45 million customer credit and debit card numbers were stolen, have ballooned to \$256 million. Those costs include detection and determination of response, internal investigation, legal and external advice, public relations and investor relations.

Media Liability: The claimant, an unsuccessful candidate for County Sheriff, alleged that a website owner allowed defamatory postings to be published on its website, which caused him to lose the election.

Media Liability: Claimant sued an online magazine alleging it published his picture without permission.

Cyber Extortion: Email sent to a leading credit card service provider threatening to cripple the site if \$10,000 ransom was not paid. After refusing to pay, the company's website went down for about a week.

Business Interruption: A computer manufacturer's plant in Ireland had to shut down after plant managers discovered a virus was loaded onto its network. Outside sources estimate the costs may have run as high as \$18.43 million.

Data Restoration: A disgruntled employee sabotaged a computer network at an investment firm and deleted files on more than 1,000 of the company's computers. It cost the company over \$3 million to assess and repair the damage.

Media Liability

Covers the insured for Intellectual Property (copyright infringement, etc.) and Personal Injury (defamation, etc.) perils that result from an error or omission in content on their website. Multimedia coverage is also available.

Cyber Extortion

Provides coverage for expenses and/or losses incurred as the result of an extortion threat made against an insured.

Business Interruption

Provides coverage for business interruption loss and/or business restoration expense incurred by the insured as the direct result of a security breach that caused system failure.

Data Restoration

Pays the reasonable costs incurred by the insured, in excess of any normal operating costs, for the restoration of any data stored.

Professional Liability

Technology E&O and/or certain miscellaneous professional liability exposures may be combined with the cyber coverage in one policy.

We take smarter care of your risk so you can take better care of your business.

Reduce your risk. Contact an advisor today.

Gallagher's Cyber Liability Practice

Corporate Headquarters

Two Pierce Place
Itasca, IL 60143
630.773.3800

Adam Cottini

Area Senior Vice President
Managing Director, Cyber Liability Practice
212.994.7048
Adam_Cottini@ajg.com

www.ajg.com/cyberliability

www.ajg.com/cyberliability

Arthur J. Gallagher & Co. at a glance

- Arthur J. Gallagher & Co. has been designing solutions to meet our clients' unique needs for more than 85 years. We pioneered many of the innovations in risk management used by businesses in all industries today. We believe that the best environment for learning and growing is one that remembers the past and invents the future.
- Founded in 1927 by Arthur J. Gallagher and still run by the founding family.
- A global corporation with a strong heritage and culture, Gallagher is a company with 20,000+ family members.
- Divisions specializing in retail insurance brokerage operations, benefits and HR consulting, wholesale distribution, and third-party administration and claims processing.
- More than 650 offices in 31 countries and revenues of \$3.6 billion.
- Offering client-service capabilities in more than 140 countries around the world through a global network of correspondent brokers and consultants.



Arthur J. Gallagher & Co.

© 2015 Arthur J. Gallagher & Co. All rights reserved.

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).

CR8BSD1115