

Frequently Asked Questions

Do you have any questions about your insurance? The frequently asked questions below are here to help you make an informed decision.

What is Cyber Insurance?

“Cyber” insurance is insurance coverage specifically designed to protect a business or organization from a range of threats and incidents relating to a breach event including:

- Liability claims involving the unauthorized release of information for which the organization has a legal obligation to keep private
- Liability claims alleging invasion of privacy and/or copyright/trademark violations in a digital, online or social media environment
- Liability claims alleging failures of computer security that result in deletion/alteration of data, transmission of malicious code, denial of service, etc.
- Defense costs in State or Federal regulatory proceedings that involve violations of privacy law; and
- The provision of expert resources and monetary reimbursement to the Insured for the out-of-pocket (1st Party) expenses associated with the appropriate handling of the types of incidents listed above

The term “Cyber” implies coverage only for incidents that involve electronic hacking or online activities, when in fact this product is much broader, covering private data and communications in many different formats – paper, digital or otherwise.

What does Privacy Liability (including Employee Privacy) cover?

The Privacy Liability aspect of the insuring agreement in our policy goes beyond providing liability protection for the Insured against the unauthorized release of Personally Identifiable Information (PII), Protected Health Information (PHI), and corporate confidential information of third parties and employees, like most popular "Data Breach" policies. Rather, our policy provides true Privacy protection in that the definition of **Privacy Breach** includes violations of a person's right to privacy, etc. Because information lost in every data breach may not fit State or Federal-specific definitions of PII or PHI, our policy broadens coverage to help fill these potentially costly gaps. This is a key provision that truly sets the BCS policy apart from others.

What does Privacy Regulatory Claims Coverage cover?

The Privacy Regulatory Claims Coverage insuring agreement provides coverage for both legal defense and the resulting fines/penalties emanating from a **Regulatory Claim** made against the Insured, alleging a privacy breach or a violation of a Federal, State, local or foreign statute or regulation with respect to privacy regulations.

Does this policy cover regulatory investigations and/or fines related to GDPR privacy violations?

The BCS cyber policy has always provided broad **Regulatory Claim** coverage that would contemplate defense and penalties associated with unintentional violations of domestic and foreign privacy statutes. In accordance with the implementation of the EU's General Data Protection Regulation, BCS added clarifying language to the policy form under the definitions of **Privacy Regulations** and **Private Information** to specifically reference coverage for GDPR by name (subject to policy terms and conditions). It is important to note that fines and penalties may not be insurable by law in certain U.S. States and in certain foreign countries, including some member countries of the European Union.

Does this policy cover regulatory investigations and/or fines related to privacy violations of the California Consumer Privacy Act (CCPA) or the Biometric Information Privacy Act (BIPA) in Illinois?

As the nature and complexity of privacy laws continues to expand across not only the U.S., but the world, the BCS policy is well positioned to address these concerns, where insurable by law. Both the California Consumer Privacy Act and the Biometric Information Privacy Act are examples of the “future-proof” nature of coverage afforded under the policy’s broad definition of **Privacy Regulations**. For instance, some insurers have issued endorsements to their policies to carve back coverage for CCPA in their anti-trust exclusions. The BCS policy has already contemplated this via carvebacks for **Regulatory Claims**, so no change of that nature is necessary. Further, some carriers have endorsed their forms to carve back coverage for CCPA in their Wrongful Collection or Gathering or Distribution of Information exclusion. No such exclusion exists in the BCS form, making an additional endorsement of this nature unnecessary. Lastly, with respect to covering the unlawful collection of, or protection of biometric information, the definition of **Private Information** in the BCS form is significantly broader than many competing forms, thus, information of this nature is inherently contemplated in the coverage.

What does Security Breach Response Coverage cover?

This 1st Party coverage reimburses an Insured for costs incurred in the event of a security breach of personal, non-public information of their customers or employees. Examples include:

- The hiring of a public relations consultant to help avert or mitigate damage to the Insured’s brand
- IT forensics, customer notification and 1st Party legal expenses to determine the Insured’s obligations under applicable Privacy Regulations
- Credit monitoring expenses for affected customers for up to 12 months, and longer if circumstances require.

The BCS policy can also extend coverage even in instances where there is no legal duty to notify if the Insured feels that doing so will mitigate potential brand damage (such voluntary notification requires prior written consent).

What does Security Liability cover?

The Security Liability insuring agreement provides coverage for the Insured for allegations of a **Security Wrongful Act**, including:

- The inability of a third-party, who is authorized to do so, to gain access to the Insured’s computer systems
- The failure to prevent unauthorized access to or use of a computer system, and/or the failure to prevent false communications such as phishing that results in corruption, deletion of or damage to electronic data, theft of data and denial of service attacks against websites or computer systems of a third party
- Protects against liability associated with the Insured’s failure to prevent transmission of malicious code from their **Computer System** to a third party’s **Computer System**

What does Multimedia Liability cover?

The Multimedia Liability insuring agreement provides broad coverage against allegations that include:

- Defamation, libel, slander, emotional distress, invasion of the right to privacy, copyright and other forms of intellectual property infringement (patent excluded) in the course of the Insured’s communication of **Media Content** in electronic (website, social media, etc.) or non-electronic forms

Other Cyber insurance policies often limit this coverage to content posted to the Insured’s website. Our policy extends what types of media are covered as well as the locations where this information resides.

What does Cyber Extortion cover?

The Cyber Extortion insuring agreement provides:

- Expense and payments (including ransom payments if necessary) to a third party to avert potential damage threatened against the Insured such as the introduction of malicious code, system interruption, data corruption or destruction or dissemination of personal or confidential corporate information.
- Ransomware is among the most reported types of cybersecurity incidents. Verizon's 2018 Data Breach Investigations Report (DBIR) indicated that ransomware is the most common type of malware, found in 39 percent of malware-related data breaches – double of the amount reported in last year's DBIR. Investigation and other expenses associated with ransomware events are contemplated under the **Cyber Extortion** insuring agreement. Additionally, Symantec's 2018 Internet Security Threat Report indicated that 2017 brought a 46% increase in new ransomware variants. Having the proper team in place to help you navigate the intricacies of a ransomware attack is critical and the BCS policy provides this through the **Cyber Extortion** coverage.

What does Business Income and Digital Asset Restoration cover?

The Business Income and Digital Asset Restoration insuring agreement provides for lost earnings and expenses incurred because of a **Network Disruption**, or, an authorized third-party's inability to access a **Computer System**. The policy will also cover for lost business as a result of a loss of reputation caused by any failure or disruption to **Computer Systems. Restoration Costs** to restore or recreate digital (not hardware) assets to their pre-loss state are provided for as well. What's more, the definition of **Computer System** is broadened to include not only systems under the Insured's direct control, but also systems under the control of a **Service Provider** with whom the Insured contracts to hold or process their digital assets. Many competing Cyber insurance forms require that a **Security Breach** take place in order for Business Interruption coverage to respond. The BCS form is unique in that the definition of **Network Disruption** is extremely broad and includes any unplanned failure, interruption or degradation of the operation of your **Computer System** or the **Computer System** of a an IT service provider – whether it was caused by a **Security Breach** or otherwise. The BCS policy further differentiates itself by taking this expansion of coverage a step further. In addition to IT service providers, coverage for **Network Disruption** is provided (on a sub-limited basis) to **Outsourced Providers**, that is, any provider, other than an IT **Service Provider**, that provides services (other than IT services) for you, pursuant to a written contract. This expanded coverage is offered without the need for additional underwriting and is sometimes referred to as "Supply Chain Business Interruption"

What is Systems Integrity Restoration coverage?

A sub-section of the **Business Income and Digital Asset Restoration** insuring agreement, **Systems Integrity Restoration Loss** provides a sub-limit for costs associated with replacement of an Insured's **Computer System** directly impacted by a **Security Compromise**.

What is "PCI-DSS Assessment" coverage?

The Payment Card Industry Data Security Standard (PCI-DSS) was established in 2006 through a collaboration of the major credit card brands as a means of bringing standardized security best practices for the secure processing of credit card transactions. Merchants and service providers must adhere to certain goals and requirements in order to be "PCI Compliant," and certain specific agreements, may subject an Insured to an "assessment" for breach of such agreements. The AJG Cyber Policy responds to **PCI Assessments** as well as claims expenses in the wake of a breach involving cardholder information. Additionally, this coverage provides for expenses associated with a mandatory audit performed by a Qualified Security Assessor (QSA), certified by the PCI Security Standards Council, to show you are PCI DSS compliant, following a **Security Breach**.

What is Cyber Deception coverage?

The **Cyber Deception** extension is purchased for an additional premium if the applicant is eligible. The extension provides coverage for the intentional misleading of the Applicant by means of a dishonest misrepresentation of a material fact contained or conveyed within an electronic or telephonic communication(s) and which is relied upon by the Applicant believing it to be genuine. This is commonly known as spear-phishing or social engineering", and, along with ransomware events, is among the most reported incidents to the BCS Cyber policy. Many Cyber policies offering this coverage require that the insured call back, or, attempt to verify the request's authenticity via a method other than the original means. In other words, if a request to transfer money to a different bank routing number is received via email, other Cyber policies may require that the person receiving the email attempt to verify the request also via telephone before authorizing the transfer of money. While the application process asks a question regarding controls in place for this, the BCS policy differentiates itself further by not requiring this of insureds in the policy wording. Additionally, this coverage provides for the loss of money from the Insured's account, or, the loss of money held on behalf of the Insured's customers or clients (aka funds held in escrow). The BCS policy does not presently offer **Cyber Deception** coverage to financial institutions or title agents.

What is Telephone Hacking coverage?

Telephone Hacking coverage is included in the **Electronic Fraud** sub-section of the BCS policy. It provides a sub-limit of coverage for the intentional, unauthorized and fraudulent use of your **Telecommunications Services** (ie: telephone, fax, broadband or other data transmission services that you purchase from third parties) that results in unauthorized calls or unauthorized use of your bandwidth.

What is Funds Transfer Fraud coverage?

Funds Transfer Fraud coverage is available in the **Electronic Fraud** sub-section of the BCS policy for insureds who are NOT classified as Financial Institutions (Financial Institutions includes Community, State or Credit Unions, as well as National Financial Institutions, Banks, etc.) or Title/Escrow/Settlement/Closing Agents or Agencies. For those organizations who are not in the Financial Institution or Title/Escrow/Settlement/Closing Agents or Agencies classifications, the coverage provides coverage for unauthorized electronic funds transfer, theft of your money or other financial assets from your bank by electronic means, theft of your money or other financial assets from your corporate credit cards by electronic means, or any fraudulent manipulation of electronic documentation while stored on your **Computer System**. This should not be confused with **Cyber Deception** coverage which requires a willful release of funds (not theft) based on a fraudulent instruction the insured believes to be true.

What is Phishing coverage?

Coverage for **Phishing Loss** is available in the **Electronic Fraud** sub-section of the BCS policy. The coverage provides reimbursement to the Insured when they are unable to collect a receivable due to them because of a third party's impersonation of them via email or other electronic means. This is often experienced when the Insured's system is compromised and a fraudster sends out an invoice, purporting to come from the Insured, however, payment routing information is changed to divert funds to the fraudster who is executing the crime. As a result, customers pay over amounts owed to fraudulent accounts, instead of to the Insured's account, and the Insured is unable to collect the monies owed to them.

What is Services Fraud Loss coverage?

Services Fraud Loss is provided in the **Electronic Fraud** sub-section of the BCS policy. “Cryptojacking” is an illegal activity on the rise whereby hackers infiltrate an Insured’s system and utilize the computing power of the network they have taken over in order to mine digital currencies. This vast increase in the infiltrators’ computing resources can lead to excessive bandwidth charges that the Insured could unknowingly incur as a result of the incident. **Services Fraud Loss** will also reimburse the Insured in the event their **Computer System** is taken over by a third party and they incur charges associated with the unauthorized use of Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), Network-as-a-Service (Naas) or IP telephony.

What is Reward Fund Loss coverage?

Also provided in the **Electronic Fraud** sub-section of the BCS policy, **Reward Fund Loss** provides reimbursement to the Insured (subject to prior underwriter consent) for monies they pay for information that leads to the arrest and conviction of any individuals committing or trying to commit an illegal act associated with a covered **Event** in the policy.

What is Personal Financial Loss coverage?

Personal Financial Loss, provided in the **Electronic Fraud** sub-section of the BCS policy, reimburses senior executive officers of the Insured for theft of money or other financial assets from their personal bank account, or identity theft of a senior executive officer, resulting from a covered **Security Breach** or **Security Compromise**.

What is Court Attendance Costs coverage?

Within the definition of **Claims Expenses**, **Court Attendance Costs** provides the Insured for reasonable sums they incur (with prior written agreement) to attend court or any tribunal, arbitration, adjudication, mediation or other hearing in connection with any covered **Claim** to which the Insured is entitled to a defense under the policy.

What is Bodily Injury and Property Damage Liability coverage?

Typically, Cyber insurance policies carry absolute exclusions for **Bodily Injury** and **Property Damage** liability. The BCS policy provides a sub-limit of coverage for liabilities associated with **Bodily Injury** and/or **Property Damage** if resulting from a **Claim** described in the **Privacy Liability** or **Security Liability** insuring agreements.

What is TCPA coverage?

The Telephone Consumer Protection Act (TCPA) is a law passed by the U.S. Congress in 1991 that amends the Communications Act of 1934. TCPA restricts telephone solicitations and the use of automated telephone equipment, automatic dialing systems, artificial or prerecorded voice messages, SMS text messages and other unsolicited means of communications. Most Cyber liability insurance policies carry a strict TCPA exclusion. The BCS policy provides a sub-limit of coverage for TCPA allegations and provides this coverage for both **Damages** and/or **Claims Expenses** – a clear differentiator in the marketplace.

What is HIPAA Corrective Action Plan coverage?

Part of the **Regulatory Liability Claims Coverage** insuring agreement, **HIPAA Corrective Action Plan Costs** are costs the Insured is obligated to pay to meet any of the requirements specified within a HIPAA corrective action plan resulting from a **Regulatory Claim** covered by the policy. Examples of costs incurred in this regard could include conducting a risk analysis, implementing risk management plans to mitigate future risk, revision of policies and procedures related to the HIPAA Security Rule, implementation of training programs and more.

What is Post Breach Response coverage?

Part of the **Breach Response Costs** definition, **Post Breach Response** provides the Insured a sub-limit of coverage (with prior consent, and utilizing pre-approved vendors) for costs incurred for the revision of an incident response plan, the completion of a network security audit, an information security risk assessment, and/or the implementation of a security awareness training program.

What is Independent Consultant coverage?

An extension of the **Business Income Loss** definition, this coverage provides for necessary costs to retain an independent consultant to determine the amount of an Insured's **Business Income Loss**.

What is Outsourced Provider coverage?

The policy provides a sub-limit of coverage for **Business Income Loss** resulting from a **Network Disruption** that occurs on an **Outsourced Provider's Computer System**. Outsourced Providers are businesses the Insured works with that perform services other than IT services, pursuant to a written contract. Also known as system failure coverage for "supply chain" partners, the coverage afforded under these terms is among the broadest in the industry.

What is Computer Hardware coverage?

Found within the definition of **Restoration Costs**, the policy will provide for reasonable and necessary costs to install a more secure and efficient version of the Insured's **Computer System** up to 25% more than the cost would have been to replace the original model, subject to a sub-limit of coverage for hardware replacement.

How is this policy better than other options in the marketplace?

As with any insurance policy, what sets our coverage apart lies in the definitions and exclusions in the policy. The BCS policy offers broader definitions of critical terms such as **Privacy Breach**, **Computer System**, and **Media Content**. Additionally, the BCS policy provides industry-leading coverage in the area of Business Interruption. These definitions, along with the absence of some industry-standard exclusions and a drastically streamlined application process, make this policy more comprehensive and easier to access than the typical Cyber policy available from traditional sources.

Isn't this already covered under most business insurance plans?

The short answer is "No". While liability coverage for data breach and privacy claims has been found in limited instances through General Liability, Commercial Crime and some D&O policies, these forms were not intended to respond to the modern threats posed in today's 24/7 information environment. Where coverage has been afforded in the past, carriers (and the ISO) are taking great measures to include exclusionary language in form updates that make clear their intentions of not covering these threats. Additionally, even if coverage can be found in rare instances through other policies, they lack the expert resources and critical 1st Party coverages that help mitigate the financial, operational and reputational damages a data breach can inflict on an organization.

Are businesses required to carry this coverage?

While there is presently no law that requires a business or organization to carry Cyber Liability Insurance, there is a national trend in business contracts for proof of this coverage. In addition, the SEC and other regulatory bodies are encouraging disclosure of this coverage as a way of demonstrating sound information security risk management. Laws such as HIPAA-HITECH, GDPR and Gramm-Leach-Bliley and state-specific data breach laws are continually driving demand as requirements for notification in the wake of a data breach become more expensive, and expectations around the level of response by an impacted organization are increased.

Do small businesses need this coverage?

A recent Ponemon Institute report uncovered that 50% of small and medium sized US businesses had suffered a data breach, with 55% suffering a cyber-attack, with the most prevalent attack being non-sophisticated phishing attempts. The US National Cyber Security Alliance has advised that 60% of small companies are out of business within 6 months after being hacked. While breaches involving public corporations and government entities garner the vast majority of headlines, it is the small business that can be most at risk. With lower information security budgets, limited personnel and greater system vulnerabilities, small businesses are increasingly at risk for a data breach. In the past, many small business owners in the SME space were reluctant to purchase Cyber liability insurance coverage because they did not see themselves as data rich targets. Today's trends are showing that much of the data breach and ransomware attacks in today's business environment are indiscriminant of industry or size. Random attacks distributed to thousands of unknown recipients with the hopes of snaring just a limited number have caused business owners of all sizes and descriptions to re-think their approach to this huge risk and purchase insurance to mitigate the effects.

If e-commerce functions such as payment processing or data storage are outsourced, is this coverage still needed?

The responsibility to notify customers of a data breach or legal liabilities associated with protecting customer data, remain the responsibility of the Insured. Generally speaking, business relationships exist between Insureds and their customers, not their customers and the back-office vendors the Insured uses to assist them in their operations. Outsourcing business critical functions such as payment processing, data storage, website hosting, etc. can help insulate Insureds from risk, however, the contractual agreement wording between Insureds, their customers and the vendors with whom they do business will govern the extent to which liability is assigned in specific incidents.