GIVE YOUR TECHNOLOGY COMPANY ADDED PROTECTION AGAINST COMMON CYBER RISKS.

Threats to cybersecurity are real. For added peace of mind, provide your tech companies with data breach, ransomware and business interruption coverage.

To demonstrate the need for these coverages, here are some claim scenarios that show the types of expenses that companies can incur.

SCENARIO 1	
Type of claim	Ransomware
Issue	Cyber extortion threat
Type of insured	Hosting/connectivity service provider
Facts	A company provides customers with hosting and connectivity solutions, including internet access, hosted environments for internal and external facing websites, hosted application services, etc. Access is restricted to authorized users through assigned user identification with user-controlled passwords. **Situation:** The company receives a threat from an unknown third party that will cause an interruption of the company's network and unauthorized access to the data stored on the company's servers. After investigating the threat, it's determined that the threat is credible and the company makes an extortion payment to the person or group making the threat. **Challenge:** The cyber extortion threat results in the following expenses for the company: • **$25,000 cyber extortion expenses**
Resolution	The total first-party expenses incurred by the service provider were $25,000.

*only if GIGA or TERA with first party data privacy endorsement

SCENARIO 2	
Type of claim	First-party data privacy loss – notification, data privacy regulatory, credit monitoring, and crisis management expenses
Issue	Breach of data privacy laws due to disabled security elements
Type of insured	Computer hardware manufacturer
Facts	A computer hardware firm manufactures network connectivity products and sells them online to customers. As part of the online transaction, nonpublic personal information is collected from customers and stored on the hardware firm's servers, which contain over 20,000 individual records. **Situation:** While conducting maintenance on the company's network, the security elements are disabled to allow applicable changes required for the network. When the network is brought back online, the security elements are inadvertently left in the disabled mode. The network is left unprotected for a period of 30 days. Although there's no evidence of a breach to the network or a compromise of the 20,000 individual records, the company has violated data privacy laws in several states and is required to notify all affected individuals of the possibility that their personal information has been exposed. **Challenge:** Even though the hardware firm doesn't receive any allegations from third parties for damages, the data privacy wrongful act results in the following expenses for the hardware firm: • **$300,000 in notification expenses** required to comply with applicable notification laws as a result of the data privacy law violation • **$700,000 in credit monitoring expenses** for individuals impacted by the breach in their nonpublic personal information • **$300,000 in legal expenses** in the defense of a data privacy regulatory proceeding that occurs as a result of the incident • **$75,000 in crisis management expenses** associated with the use of a crisis management firm to minimize the potential harm to the hardware company from the data privacy wrongful act
Resolution	The total first-party expenses incurred by the hardware manufacturer were in excess of $1.3 million.

*only if GIGA or TERA with first party data privacy endorsement

SCENARIO 3	
Type of claim	First-party data privacy loss – notification, credit monitoring and cyber investigation expenses
Issue	Improper disclosure of nonpublic personal information
Type of insured	Software developer
Facts	A software developer manufactures and distributes workforce management software that allows third parties to track employee hours, overtime, vacation time and compiles information for payroll processing. The software is offered on a "Software as a Services" (SaaS) model that allows the developer to provide customers with access and use of the applications through a hosted environment, including storage of customer data on a server controlled by the developer. **Situation:** Unauthorized access to this data results in the improper dissemination of nonpublic personal information for 1,000 individuals and violates data privacy laws in several states. **Challenge:** Although the software developer doesn't receive any allegations from third parties for damages, the data privacy wrongful act results in the following first-party expenses for the developer: • **$15,000 in notification expenses** required to comply with applicable notification laws as a result of the data privacy law violation • **$35,000 in credit monitoring expenses** for individuals impacted by the breach in their nonpublic personal information • **$7,500 in cyber investigation expenses** to hire a company to investigate the cause of the security breach
Resolution	The total first-party expenses incurred by the software developer were in excess of $50,000.

*only if GIGA or TERA with first party data privacy endorsement

SCENARIO 4	
Type of claim	First-party data privacy loss – notification and credit monitoring expenses
Issue	Lost data tape
Type of insured	Custom software developing and consulting
Facts	A software consultant firm provides advice and services related to the implementation of database software applications. They also provide logistics applications used by businesses to manage their operations, including reporting tools. Additionally, the company provides data transfer services, which may include the handling and use of data tapes. **Situation:** When working on a recent project, the company receives a backup copy of customer data on magnetic tape. After completing the project, it's discovered that this backup data tape: • Included nonpublic personal information for thousands of individuals • Cannot be accounted for **Challenge:** Although the hardware firm doesn't receive any allegations from third parties for damages, the data privacy wrongful act results in the following expenses for the software consultant firm: • **$30,000 in notification expenses** required to comply with applicable notification laws as a result of the data privacy law violation • **$70,000 in credit monitoring expenses** for individuals impacted by the breach in their nonpublic personal information
Resolution	The total first-party expenses incurred by the custom software developer were $100,000.

*only if GIGA or TERA with first party data privacy endorsement

SCENARIO 5	
Type of claim	Business interruption
Issue	Ransomware attack
Type of insured	Technology manufacturer
Facts	A technology manufacturer assists engineers in providing them the data capabilities they need to turn their innovative ideas into a reality. **Situation:** The manufacturer suffered a ransomware attack and then sought council from The Hartford on how to proceed. **Challenge:** Insured did not pay ransom and instead requested The Hartford reimburse them for the following costs incurred as a result of the incident: $867,000 - Business Interruption Costs $40,175 - Forensic Expenses $3,960 - Legal Costs $112,536.68 - Other Data Restoration and Related Expenses
Resolution	After review, the expenses were reimbursed in full to the insured, who had a policy under Tech E&O with a First Party Expense endorsement. This endorsement covers both business interruption loss and data restoration.

*only if GIGA or TERA with first party data privacy endorsement

DISCOVER OUR FULL RANGE OF PRODUCTS AND SERVICES

at **TheHartford.com/technology**

And get additional information on our cyber coverage and how it can benefit your clients at the links below:

Coverage Analyzer | **Cyber Services Portfolio** | **Cyber Center**

THE HARTFORD

Business Insurance
Employee Benefits
Auto
Home