TRAVELERS

PRE POST ALWAYS

PROTECTION FROM EVERY ANGLE

CyberRisk | COVERAGE HIGHLIGHTS FOR NONPROFIT ORGANIZATIONS

WHY YOU NEED THE PROTECTION

It takes only one cyber event or data security breach to impair your company's financial results, or even potentially put you out of business. One resourceful hacker, virus, or system glitch can shut down your entire network within minutes, paralyzing operations and your ability to earn income. One successful hack, lost laptop, or lost paper record can cause a data breach impacting the privacy of customers, employees, and others. Travelers has you protected from every angle... pre-breach, post-breach and always.

COVERAGE HIGHLIGHTS

CyberRisk coverage is specifically designed to help in the event of a cyber breach. It's available for businesses of all sizes as a stand-alone policy or as part of a management liability suite of coverages. CyberRisk provides more solutions with options that include coverage for forensic investigations, litigation expenses associated with the breach, regulatory defense expenses/fines, crisis management expenses, business interruption and cyber extortion. And now, CyberRisk protection doesn't end after a breach occurs. New to CyberRisk is Betterment – an insuring agreement that provides coverage for costs to improve a computer system after a security breach, when the improvements are recommended to eliminate vulnerabilities that could lead to a similar breach. In addition to coverage, Travelers provides policyholders innovative value added pre-breach and post-breach risk management services at no additional cost.

These include access to Travelers pre-breach services provided by Symantec™, a global leader in cybersecurity solutions. Services include a Cyber Resilience Readiness Assessment and Consultation, Security Coach Helpline, Cyber Security Awareness training videos and much more. Policyholders also receive access to Travelers' eRiskHub® – an information portal that includes pre-breach and post-breach benefits such as:

- Tools to build privacy controls, information and IT security programs
- Calculators to estimate potential costs of an event
- Breach Coach®, Privacy Coach and Security Coach consultations
- Listing of experts who help customers build/improve cyber programs
- Sample incident roadmap for dealing with a breach
- Easy access to Travelers' claim reporting website

TRAVELERS CYBERRISK COVERAGE INCLUDES THE FOLLOWING INSURING AGREEMENTS:

Liability Insuring Agreements:

PRIVACY AND SECURITY
Coverage for claims arising from unauthorized access to data, failure to provide notification of a data breach where required by law, failure to destroy confidential information, failure to comply with a privacy policy, wrongful collection of private or confidential information, failure to prevent a security breach that results in the inability of authorized users to gain system access, the participation in a DDoS attack, or the transmission of a computer virus.

MEDIA
Coverage for claims arising from copyright infringement, plagiarism, defamation, libel, slander, and violation of an individual's right of privacy or publicity in electronic and printed content.

REGULATORY
Coverage for administrative and regulatory proceedings, civil and investigative demands brought by domestic or foreign governmental entities or claims made as a result of privacy and security acts or media acts.

Breach Response Insuring Agreements:

PRIVACY BREACH NOTIFICATION
Coverage for costs to notify and provide services to individuals or entities who have been affected by a data breach. Examples include call center services, notification, credit monitoring and the cost to purchase identity fraud insurance.

COMPUTER AND LEGAL EXPERTS
Coverage for costs associated with analyzing, containing, or stopping privacy or security breaches; determining whose confidential information was lost, stolen, accessed, or disclosed; and providing legal services to respond to such breaches.

BETTERMENT
Coverage for costs to improve a computer system after a security breach, when the improvements are recommended to eliminate vulnerabilities that could lead to a similar breach.

CYBER EXTORTION
Coverage for ransom and related costs associated with responding to threats made to attack a system or to access or disclose confidential information.

DATA RESTORATION
Coverage for costs to restore or recover electronic data, computer programs, or software lost from system damage due to computer virus, denial-of-service attack or unauthorized access.

PUBLIC RELATIONS
Coverage for public relations services to mitigate negative publicity resulting from an actual or suspected privacy breach, security breach, or media act.

Cyber Crime Insuring Agreements:

COMPUTER FRAUD
Coverage for loss of money, securities, or other property due to unauthorized system access.

FUNDS TRANSFER FRAUD
Coverage for loss of money or securities due to fraudulent transfer instructions to a financial institution.

SOCIAL ENGINEERING FRAUD
Coverage for loss of money or securities due to a person impersonating another and fraudulently providing instructions to transfer funds.

TELECOM FRAUD
Coverage for amounts charged by a telephone service provider resulting from an unauthorized person accessing or using an insured's telephone system.

Business Loss Insuring Agreements:

BUSINESS INTERRUPTION
Coverage for loss of income and expenses to restore operations as a result of a computer system disruption caused by a virus or computer attack, including the voluntary shutdown of systems to minimize the business impact of the event.

DEPENDENT BUSINESS INTERRUPTION
Multiple coverage options for loss of income and expenses to restore operations as a result of an interruption to the computer system of a third party that the insured relies on to run their business.

SYSTEM FAILURE
Coverage for loss of income and expenses to restore operations as a result of an accidental, unintentional, and unplanned interruption of an insured's computer system.

REPUTATIONAL HARM
Coverage for lost business income that occurs as a result of damage to a business' reputation when an actual or potential cyber event becomes public.

TRAVELERS

Available through the Travelers *Wrap+*℠ and *Executive Choice+*℠ suite of products.

TRAVELERS

CyberRisk | CLAIM SCENARIOS FOR NONPROFIT ORGANIZATIONS

A CyberRisk policy can help protect against data breaches and other fast-evolving cyber exposures not covered by standard property and liability policies. Travelers CyberRisk policy responds in multiple ways such as security card data remediation and notification expense, network and information security liability, regulatory defense expenses, crisis management event expenses, and computer program and electronic data restoration expenses.

INSIDER BREACH

A A nonprofit Labor Union Plan was responsible for a data privacy breach when one of their employees sent a company file to her personal email account, which contained the names, addresses, social security numbers and financial information of 500 union members. Federal law enforcement notified the Labor Union Plan that union members' personally identifiable information was used to file fraudulent tax returns. Upon learning of this event the Labor Union Plan fired the employee, had to notify the 500 clients of the data breach, provide credit monitoring to the 500 members and set up a call center to handle various inquiries. According to the NetDiligence® Data Breach Cost Calculator* the estimated costs to the nonprofit Labor Union Plan could be $191,000.

WEBSITE VULNERABILITY

A metropolitan food bank service experienced a cybersecurity breach that resulted in the inadvertent disclosure of more than 10,000 donors' personal information. Due to malware on their website server the unauthorized individual was able to gain access to donor information over a three year period. The personal information included names, addresses, emails, credit and debit card numbers, security codes and expiration dates. Computer forensic experts were retained to assist with the investigation. Corrective measures were taken including changing all passwords, implementing additional monitoring and reviewing the food bank's policies and procedures to ensure that all information was appropriately protected moving forward. In addition, due to the various state laws that had been implicated, the food bank was required to notify all affected donors and provide identity protection and credit monitoring

for a one year period. According to the NetDiligence® Data Breach Cost Calculator* the estimated costs for this event for the food bank could be $900,000.

HACKER EVENT

A cybercriminal hacked into a nonprofit Chamber of Commerce network through an unprotected server and gained access to employee records. After discovering the incident, the Chamber of Commerce immediately shut down its server and retained a computer forensic expert to further investigate. The investigation determined that the attacker had gained access to 325 records of past and present employees which included names, Social Security numbers, birth dates, addresses, and bank account information. In compliance with state guidelines, the 325 employees were notified and credit monitoring was offered. According to the NetDiligence® Data Breach Cost Calculator* the estimated costs for this event for the nonprofit Chamber of Commerce could be $186,000.

In addition to these costs, the Betterment insuring agreement could pay for costs to improve the insured's computer system to eliminate vulnerabilities that could lead to a similar breach.

MISUSE OF PERSONALLY IDENTIFIABLE INFORMATION

A nonprofit K-12 school sent out letters to 5,000 parents notifying them of some new curriculum guidelines. Inadvertently each student's social security number was printed as part of the address field on the outside of each envelope. This exposure is considered a violation of each student's Personally Identifiable Information (PII). As a result, the school was required to notify each family of the event and provide one year of identity protection and credit monitoring. According to the NetDiligence® Data Breach Cost Calculator* the estimated costs for this event for the nonprofit K-12 school could be $312,000.

STOLEN LAPTOP

The treasurer of a nonprofit organization stopped off at the local grocery store on his way home from work. While he was shopping his car was broken into and his laptop was stolen. The laptop contained private financial information belonging to the nonprofit organization's donors. Personal information, credit card data and even bank account numbers of 1,000 donors were compromised. When the donors found out about the breach they filed a lawsuit against the nonprofit organization for damages resulting from the alleged failure to protect their private financial information. According to the NetDiligence® Data Breach Cost Calculator* the estimated costs for this event for the local nonprofit organization could be $748,000.

WHY TRAVELERS?

- We've provided effective insurance solutions for more than 160 years and address the needs of a wide range of industries
- We consistently receive high marks from independent ratings agencies for our financial strength and claims-paying ability
- With offices nationwide, we possess national strength and local presence
- Our dedicated underwriters and claim professionals offer extensive industry and product knowledge

Travelers knows CyberRisk.

To learn more, talk to your independent agent or broker, or visit travelers.com/cyber.

* The NetDiligence® Data Breach Cost Calculator and other tools are available to insureds on the Travelers' *eRisk Hub®*. eRisk Hub is a registered trademark of NetDiligence.

TRAVELERS

Available through the *Travelers Wrap+®* and *Executive Choice+®* suite of products.

travelers.com