Cyber Risk Management & Insurance Overview

Contents

Aon CyberBusinessPro[sm] is the nation's premier cyber insurance and risk management suite empowering small businesses to better ***prevent, protect against and respond*** to cybercrime. The program is aimed at addressing what most small businesses need, which is an affordable solution that delivers essential risk management tools to mitigate exposures, 24/7 access to experts to respond to incidents and the financial protection provided by A-rated insurers.

Prevent - Essential Risk Management

Small businesses face an array of cyber security challenges daily. CyberBusinessPro includes important risk management tools tailored for small businesses. Best practices, compliance and contractual obligations require prevention practices to help address and mitigate cyber risks. With CyberBusinessPro, depending on the limit of insurance you secure, you can take advantage of the following benefits:

24/7 Tech Support Hotline

Tech support for your office is just a phone call away! Remote support allows users to get technical problems resolved immediately and affordably. Support is provided for more than just computers. Technicians are available 24 hours a day, 7 days a week to help resolve the following types of issues:

- Diagnostics
- Basic Network Setup & Support
- PC & Mac Maintenance & Optimization
- Virus & Spyware Removal
- Data Backup Assistance

- Operating System Issues
- Software Setup & Troubleshoot
- Printers & Scanners Support
- Internet & Email Issues
- WiFi & Router Setup
- & More!

Aon CyberBusinessPro[SM]
DATA EXPOSURE RESPONSE PROTECTION

Keystroke Encryption Software

Keystroke Encryption Software helps protect your identity and sensitive business activities by encrypting your computer keystrokes and hiding them from hackers, malware and keylogger's intent on stealing your sensitive credentials while using the internet.

Human Resources Module

Aon CyberBusinessPro includes unlimited access to education and training that focuses on cyber security, privacy and identity theft. Applicants, employees and managers each have separate levels of modules.

Risk Assessments / Written Policies / Templates / Incident Response Plan

To support information security efforts, we provide our guides, templates and self-assessments for your unlimited use. We understand that information security is complex and that some companies are just beginning their information security efforts, while others are more mature. That's why we provide our self-assessment protocols in four distinct levels, Beginner I/II, Intermediate and Advanced. Because not all businesses have the same exposures or experience, our protocols are designed to add value and meet your specific level of need.

"CyberBusinessPro's cyber solutions were created to deliver the peace of mind, resources and insurance protection you need to reinforce your prudence and to help ensure you survive a cyber incident."
—Tom Widman, Program Administrator

Dark Web Monitoring

Industry leading technology that scans the dark web providing threat intelligence relating to your organization and/or industry.

Computer Vulnerability Scans

Identify vulnerabilities on your computer before hackers do.

Protect - Cyber Insurance Coverage

Does your small business collect, use and/or disclose personal information? Do you operate a website? If so, it is entirely appropriate to have insurance to defend and cover the specialty cyber, privacy and information related liability exposures that exist. When it comes to cyber risks, our primary message is "*Do your best, and insure the rest*". We understand that protecting computers and information against loss or theft is difficult. Because cyber risks will always remain, no matter how diligent your defenses, insurance presents a cost effective vehicle to transfer risk. We believe that cyber liability insurance is a fundamental need of every business, especially in today's risk environment.

Privacy & Security Cyber Liability Insurance

Coverage is provided for a theft, loss or unauthorized disclosure of protected information in the care, custody or control of the insured or third party which the insured is legally responsible for; Failure to notify a third party in violation of a privacy law.

Cyber Extortion / Ransomware

Ransomware, one of the fastest growing areas of cyber crime, refers to malicious software that is specifically designed to take control of a computer system or its data and hold it hostage so the attackers can demand payment from their victims.[1]

Dependent eNetwork Interruption

In the interconnected global economy, a company's business may rely on the operations and products/services of another company (think of an Auto Manufacturer relying on the supply of steel for the production of vehicles, or an online retailer relying on the functionality and dependability of a 3rd parties hosting platform). Dependent Business Interruption loss, also known as Contingent Business Interruption loss occurs as the insured is unable to access the necessary materials or services which support the insured's operations (raw materials, website functionality, cloud service provider, etc.), thus impacting revenues.

eNetwork Interruption (Business Interruption) & Data Reconstruction

A network interruption loss happens when a cyber-event causes a disruption in the operations of a company, which results in lost business revenue. Some of the more common cyber-attacks against businesses which may lead to a NI Loss include denial-of-service, insertion of malware or malicious code, and ransomware.

Expanded Liability

Coverage for cyber events to include i) an unintentional and unplanned interruption of any computer system; ii) the storage, collection, use or disclosure of Protected Information that is in violation of a Privacy Law.

Incident Response / Breach Costs

Coverage for law firm/breach coach, PR firm, forensics, consumer notifications and remedies for identity theft education and assistance, victim cost reimbursement insurance, and credit file or identity monitoring.

Media Liability

This is a risk faced by many companies who create or disseminate information either electronically or physically. Risk is usually driven through the following areas: defamation, libel/slander, invasion of privacy, infringement of copyright and trademark, and plagiarism.

Payment Card Industry (PCI)

A company (merchant) which accepts credit cards and has signed a Merchant Services Agreement (MSA) with their bank has an obligation to safeguard payment card data. If such merchant experiences a security breach involving payment card (PCI) data and is found to be non-compliant with PCI rules, they may be subject to PCI-DSS Fines and PCI-DSS Assessments, and are required to indemnify their bank for costs incurred.

Regulatory Fines & Penalties

Costs for defending against regulatory actions and resulting fines and penalties arising from a covered privacy event

Social Engineering & eCrime

Also known as Fraudulent Wire Transfer Loss, a social engineering scheme is accomplished by tricking an employee of a company into transferring funds to a fraudster.

The fraudster sends an email impersonating a vendor, client, or supervisor of the company and advises that banking information for the vendor/client has changed or company funds immediately need to be wired at the "supervisor's" direction. The email looks authentic because it has the right logos and company information and only careful study of the email will reveal that the funds are being sent to the fraudster's account. Unsuspecting and trusting employees unwittingly have cost their companies millions of dollars in connection with social engineering claims.

System Failure & Bricking

Lost income arising from system failure and reputation loss (future income loss). "Bricking" provides for the cost to repair or replace computer hardware or equipment that is damaged or impaired and must be replaced.

Telephone Hacking

Telephone Toll Fraud involves the hijacking of a phone system over the Internet to dial out to premium numbers in distant countries at several dollars a minute.

Additional benefits available from CyberBusinessPro

CEO Personal Identity Protection

Automatic CEO identity protection includes VRS (Victim Resolution Services) Elite Unlimited fraud victim resolution services combined with $15,000 identity insurance. No enrollment necessary.

Respond - Incident Response On-Demand™

Having an elite team of experts available via our **Incident Response On-Demand**™ is indispensable when faced with a cyber catastrophe or cyber event. Whether the business has 5 customers or 5 million, our capabilities to respond to a cyber incident are seasoned and flexible. Our team of experts will seek to assess and contain the loss, preserve evidence, and support continuity of the business. Experienced in data forensics, investigators have the ability to support law enforcement and pursue independent investigations, while our notification, victim assistance and identity protection monitoring programs can be activated nationwide within 24-hours.

Aon **CyberBusinessPro**℠
DATA EXPOSURE RESPONSE PROTECTION