The Hanover Insurance Group®

Hanover Cyber Advantage

Hanover Cyber Advantage Premier coverage scenarios

With cyber threats constantly evolving, businesses need a flexible cyber insurance solution that can respond to the ever-changing exposures. Through Hanover Specialty Insurance Brokers (HSIB), our in-house excess and surplus brokerage, we offer Hanover Cyber Advantage Premier, a non-admitted stand-alone cyber solution that provides robust cyber protection against traditional and emerging risks. These scenarios help to show you how.

Coverage

RISK EXPOSURE	KEY QUESTION	THE HANOVER SOLUTION
Data breach	How would a business be impacted if a network was violated by a hacker and clients' personally identifiable information was exposed?	Our **privacy and security liability** covers multiple types of expenses associated with a cyber breach, including breach restoration, cyber investigation, business interruption/extra expense, cyber extortion and cyber theft. Additionally, we provide third-party liability related to mishandling a client's personal information, including a cyberattack on a firm's system, actions of a rogue employee, violations of customer notification laws and more.
Social engineering	What would happen if a fraudster impersonates a vendor and tricks an employee into voluntarily transferring several payments?	Our **social engineering fraud coverage** covers the loss of money or securities resulting from a social engineering event where a third-party pretends to be a client, vendor, employee or executive officer and persuades a business to transfer money or send securities.
Consumer reparations	What would happen if a business is obligated to deposit funds in a redress fund?	Our **regulatory proceeding coverage** definition includes coverage for consumer redress funds as a result of an information security breach following a privacy and security wrongful act.
Business interruption	How would a business be affected by lost revenue because a denial-of-service attack prevents it from doing business?	Our **contingent business income loss and extra expense coverage** covers lost business income and extra expenses a business incurs while its system is being restored following a cyberattack. Our coverage also covers public relations service expenses to help a business protect its reputation.
Loss of revenue	What would happen if a business has its systems fully restored after an attack but revenue does not immediately return to its pre-attack level, because customers are hesitant to return?	Our **reputational harm coverage** provides coverage for the reduction in revenue after a business's system is restored following an attack. This protection goes beyond traditional business income coverage which provides coverage only until the system is restored.
Inoperable hardware	What would happen if a malware attack renders all of a business's laptops unusable, requiring total replacement?	Our **hardware replacement expense coverage** covers the expenses to replace hardware that has been rendered inoperable or "bricked" by a malicious attack.
Digital currency fraud	How would a business be affected if large sums of digital currency were transferred to an unintended account due to fraudulent instructions?	Our definition of money includes **digital currency** and would provide coverage for instances in which an intentional, unauthorized and fraudulent instruction directs the business's funds to an account to which it did not intend to transfer.
System resources fraud	What would happen if a business incurred significant additional utility expenses because a hacker used its computing resources to mine digital currency?	Our **systems resource fraud coverage** provides coverage for the increased utility expenses that occur when a third-party maliciously gains access to a business's network in order to use its computing power to their benefit, such as in the case of mining digital currency.

RISK EXPOSURE	KEY QUESTION	THE HANOVER SOLUTION
Post-cyberattack system vulnerabilities	Would a business have funds available to address system vulnerabilities when also dealing with the fallout of a cyberattack?	Our **systems remediation coverage endorsement** provides funds to help address the vulnerabilities and secure a system after a loss to help prevent future incidents. Traditional systems remediation coverage would only pay for a business to mitigate the fallout of a cyberattack.
Pollution event	How would a manufacturer respond if a third party gained access to its process control systems and redirected pipes carrying controlled substances, resulting in a pollution leak?	Our **pollution expense coverage** provides coverage for an actual and sudden discharge, seepage or release of pollutants. This coverage is important for businesses that are working with high-hazard chemicals or liquids and have connected systems that are vulnerable to an attack.
Data manipulation	What would happen if a business was unable to collect payments from customers because invoices were manipulated?	Our **computer fraud coverage** provides protection for events that are related to the unauthorized manipulation of data within a business's computer system causing loss of money, securities, or other property. Our definition is also enhanced to cover for invoice manipulation resulting in your inability to collect payment for goods, products, or services after they have been transferred to the customer.

Service

RISK EXPOSURE	KEY QUESTION	THE HANOVER SOLUTION
Data security, profitability and reputation	What assistance is available to help a business understand existing and emerging hazards and prevent potential losses?	We have partnered with NetDiligence®, an expert cyber risk assessment and data breach services company, to provide access to tools and resources to help understand exposures, establish a response plan and minimize the effects of a breach, via the eRisk Hub® Portal.
Managing the effects of a cyberattack	What assistance is available to help a business quickly and skillfully respond to a cyber incident?	We have partnered with industry-leading legal counsel, forensic IT, data recovery and breach response experts to provide businesses with preferred access and pricing for their services. Our partners are standing by, ready to provide trusted guidance, reassuring support and a broad range of response and remediation services.

Learn more

For more information about Hanover Cyber Advantage Premier, contact Hanover Specialty Insurance Brokers at CyberQuote@hanover.com.

The Hanover Insurance Group®

Hanover Specialty Insurance Brokers
10480 Little Patuxent Parkway, Suite 500
Columbia, MD 21044

hanover.com
The Agency Place (TAP)—https://tap.hanover.com

119-10078 (1/20) LC 2019-365