CRC Group
Wholesale & Specialty

INSUREtrust

WHY BUY CYBER INSURANCE?

In our increasingly digital world, a company's protection of its core digital assets has become essential. Moving well beyond traditional data breaches and theft of critical or sensitive information, cyber risk can bring a company's operations to a standstill, threatening significant loss of revenue and eroding confidence with clients and customers.

Cyber insurance is a key component of any comprehensive risk management strategy for businesses of all sizes and provides several critical benefits, including:

1 | FINANCIAL PROTECTION

Cyber incidents can be extremely costly, involving expenses related to data breach notification, data recovery, legal fees, ransomware events (including payments), defense costs, and potential fines, settlements, or damages. Cyber insurance can provide financial coverage for these expenses, helping to mitigate the impact of a cyber event.

2 | BUSINESS CONTINUITY

Cyber attacks, such as ransomware, can disrupt business operations and lead to significant financial losses. Cyber insurance can cover the loss of income and extra expenses during downtime, helping businesses maintain financial stability and continuity of operations.

3 | CYBER CRIME

Cyber carriers cite today's leading cause of loss as social engineering, which is the wrongful transfer of money due to fraudulent payment instructions. A properly structured cyber policy can go beyond paying for traditional data breaches and cyber attacks; it can also extend to several aspects of commercial crime loss (including social engineering).

4 | COMPLIANCE REQUIREMENTS

Many industries are subject to regulations that require businesses to protect, handle, manage or delete data in a specific manner. Cyber insurance policies can provide coverage for regulatory fines and penalties, as well as the costs associated with compliance investigations, inquiries, and audits.

5 | RISK MANAGEMENT SUPPORT

Beyond financial compensation, cyber insurance providers often offer risk management services to help businesses improve their cybersecurity posture. Risk assessments, employee training programs, and security improvement recommendations are just a few examples of services that can help reduce the likelihood of a cyber incident and can improve an organization's risk profile for cyber underwriters.

6 | ACCESS TO EXPERTISE

Cyber insurers typically offer access to a network of cybersecurity professionals. Incident response experts can assist in the immediate aftermath of a cyber incident, providing services such as forensic analysis, legal advice, and crisis management, which are vital for a quick and effective response. These services often come at discounted rates compared to the rates paid by uninsured companies.

7 | ADDRESSES NEW TECHNOLOGIES

As the digital age moves forward and as organizations adopt emerging technology like artificial intelligence, cyber underwriters are actively exploring how to provide coverage and enhance protection for insureds. The cyber insurance application and underwriting process can also provide unique insights into these innovative technologies.

8 | SUPPLY CHAIN PROTECTION

Many organizations rely on outsourced parties to fulfill a variety of functions and services on their behalf. Organizations may fall victim to cyber losses due to the fault of a third party, and most cyber insurance policies provide coverage for such losses while also seeking indemnification from the at-fault party.

9 | BOARD LEVEL SUPPORT

Directors and Officers have an obligation to protect their organization from devastating cyber events. Cyber insurance can aid in the cross-discipline understanding and protection from cyber risks, while also safeguarding the company's assets.

10 | REPUTATION MANAGEMENT

A cyber attack can significantly damage a company's reputation. Cyber insurance often includes access to public relations experts and crisis management services to help manage and mitigate reputational damage following a breach.

Cyber risks are consistently increasing in severity, sophistication, and frequency. Organizations need to adapt quickly to address the changing landscape by identifying, prioritizing, and managing cyber exposures as a part of their overall cyber risk strategy. An integral part of this process is purchasing cyber insurance—it is a "belt-and-suspenders" approach to other proactive cyber risk mitigation strategies. Not only does cyber insurance serve as a financial backstop to manage emerging risks, but the available risk management services offered can provide valuable resources and solutions for organizations with varying degrees of cyber sophistication. Cyber insurance has grown into a risk management solution that all companies should consider.

Cyber insurance can aid in the cross-discipline understanding and protection from cyber risks, while also safeguarding the company's assets.

CRC/INSURETRUST CYBER PRACTICE GROUP

SUMMARY OF CYBER INSURING AGREEMENTS

First Party Coverage:

Cyber Incident Response Costs (some policies provide outside of the policy limit):

• Legal Counsel

Generally the first connection made between the insured and claims representation is with the insured's assigned incident response attorney ("breach coach") who will act as the point of contact and provide legal advice on responding to a cyber event or potential cyber event. Will also advise on additional vendors needed and will direct those engagements so as to preserve attorney-client privilege.

• Digital Forensics Incident Response

Coverage to pay for the hiring of a forensics firm to investigate the scope and severity of a cyber incident.

• Crisis Management and Public Relations

If necessary, to minimize damage to reputation, a public relations firm should be hired to coordinate internal and external communication following a cyber event.

• Notification Costs, Credit Monitoring and Identity Restoration

If necessary, notification of affected individuals should take place in accordance with each state's (or foreign jurisdiction's) notification laws, as well as offer credit monitoring and identity restoration reimbursements. Some policies allow coverage for voluntary notification as well.

• Business Interruption

Coverage for lost profit, continuing operating expenses and extra expenses the insured incurs while being shut down either due to a hacking event (**security failure** – i.e. ransomware, malicious code, Denial of service attack) or an interruption or unplanned outage (**system failure** - i.e. human or operational error, coding error).

• Voluntary Shutdown

Some policies extend business interruption coverage when an insured has to voluntarily pull their network offline to prevent an attack

• Proof of Loss

Coverage for the insured to engage a forensic accounting firm to help them create a proof of loss during the claim process.

• Dependent Business Interruption

Coverage for lost profit, continuing operating expenses and extra expenses the insured incurs while being shut down but if the event occurs at a third party that provides services to the insured under written contract. Can be due to a system failure or security failure.

• Dependent Business Interruption Vendor Types

Types of vendors that dependent business interruption coverage extends to:

- **IT Providers only:** Only those vendors that provide IT services to the insured under written contract.
- **IT and BPO Providers:** Only those vendors that provide IT services or business process outsourcing services to the insured under written contract**.**
- **All contracted providers:** All vendors that have a written contract with the insured other than ISPs, utilities, and security exchanges.

Any Business Interruption coverage typically has a waiting period which denotes the period of time that must elapse before the coverage is effective.

• Data Restoration

Coverage to recover or restore data lost in a security failure or privacy event.

• Bricking

Some policies provide coverage for the replacement of hardware as the result of a security failure that renders the hardware useless.

• Cyber Extortion

Coverage to pay for the investigation or potential ransom to an attacker who is threatening to release data or has control of the insured's network.

CRC/INSURETRUST CYBER PRACTICE GROUP

SUMMARY OF CYBER INSURING AGREEMENTS

Cyber Crime:

• Social Engineering Coverage

Coverage when the insured is tricked into transferring money (or products where noted) to a 3rd party while believing they are transferring to a legitimate vendor or customer.

• Invoice Manipulation

Coverage when the insured's network is breached and a fraudulent invoice is sent out to a legitimate customer or vendor. That customer or vendor then pays the fraudster, leaving the insured with an uncollectible receivable.

• Funds Transfer Fraud

Coverage for loss of funds by the insured due to fraudulent instructions issued to their financial institution by somebody other than an insured.

• Telecom Fraud

Coverage for misappropriation of an insured's telephone or fax system by attackers that results in an increased telecom bill.

• Cryptojacking/Utility

Coverage for theft of computer or utility resources resulting from a breach of the insured's network.

Third Party Liability Coverage (includes damages and defense costs):

• Network Security and Privacy

Liability coverage for breach of the network or wrongful release or theft of confidential information.

• Theft of all Forms of Data Covered

Protection for the insured for the disclosure of data in any form. Note to whether biometric data is covered.

• Regulatory Fines and Penalties

Coverage to respond to a regulatory inquiry and the associated fines by a governmental entity resulting from a disclosure of confidential information in violation of a privacy law (GDPR, CCPA, HIPAA).

• PCI DSS Fines and Penalties

Coverage for assessments brought by card brands arising from a release of PCI (payment card industry) data.

• Wrongful Collection

Coverage for the improper collection of data in violation of privacy laws.

• Digital and Non-Digital

Liability coverage for content and intellectual property claims arising from the insured's use of digital and non-digital media or only digital media.

Policies should protect the innocent insured company in the event a cyber incident was the result of dishonest employee (i.e. rogue employee coverage). Does not include acts by owners/officers.

The **CRC/INSUREtrust Cyber Practice Group** combines CRC's capabilities as one of North America's largest wholesale specialty insurance distributors with INSUREtrust's exclusive products and extensive experience. Dedicated to addressing evolving cyber insurance needs with innovative tailored solutions for the modern business environment, the group offers best-in-class cyber brokerage, products, risk management, and education for the retail insurance community.

Please contact your CRC / INSUREtrust Producer to learn more.