INSURETRUST TEAM - CRC 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.

INSURETRUST TEAM - CRC 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.

Please contact your CRC INSUREtrust Team Producer to learn more.