Cyber Insurance Policy Coverage Checklist

LIABILITY COVERAGES

- [ ] **Network Security & Privacy Liability**: liability coverage for a breach of the network or wrongful release of confidential information
- [ ] **Breach of Privacy Statement**: protection for the insured in the event they are non-compliant with their corporate privacy policy
- [ ] **Regulatory Fines & Penalties**: coverage for fines by a governmental entity resulting from the disclosure of confidential information in violation of privacy law (GDPR, CCPA, HIPAA)
- [ ] **PCI Fines & Penalties**: coverage for assessments made by card brands arising from a release of PCI (payment card industry) data
- [ ] **Wrongful Collection of Private Information**: coverage for the improper collection of data in violation of privacy laws
- [ ] **Theft of All Forms of Data Covered (including Biometric)**: protection for the insured for the disclosure of data in any form
- [ ] **Rogue Employee Coverage**: protection for the innocent insured in the event a data breach was the result of a dishonest employee. Does not include acts by owners/officers.
- [ ] **Digital & Non-Digital Media**: liability coverage for content intellectual property claims arising from the insured's use of digital and non-digital media or only digital media

CYBER CRIME

- [ ] **Social Engineering**: 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
- [ ] **Social Engineering Authentication requirement**: Is there a provision in the policy in which social engineering coverage only applies to insureds who provide a means of second verification that the wire funds transfer is legitimate before sending the money?
- [ ] **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**: 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 Fraud**: coverage for theft of computer or utility resources resulting from a breach of the insured's network

MIS

PROTECTING YOUR WORLD
BURNETTE
INSURANCE
EST. 1971

Stan Burnette
Burnette Insurance
770-339-8888
stan@burnetteinsurance.com

FIRST-PARTY COVERAGES

- [ ] **Ransomware/Cyber Extortion**: coverage to pay for the investigation and potential ransom to an attacker who is threatening to release data or has control of the insured's network
- [ ] **Legal Advice/Breach Coach**: Generally, the first connection made between the insured and claims representation is with the insured's assigned breach coach who will act as the point of contact and provide legal advice on responding to a cyber event or potential cyber event.
- [ ] **Forensics Costs**: coverage to pay for hiring a forensics team to investigate the scope of a cyber incident
- [ ] **Crisis Management & Public Relations Costs**: To minimize reputational damage, a public relations firm should be hired to coordinate internal and external communication following a cyber event.
- [ ] **Notification Costs, Credit Monitoring & 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
- [ ] **Notification & Credit Monitoring Outside the Limit**: coverage for Notification Costs & Credit Monitoring are outside the policy limit
- [ ] **Outside the Limit:** coverage for all incident response (legal advice, forensics, public relations, notification and credit monitoring) are provided outside the policy limit
- [ ] **Business Interruption Security Failure**: coverage for lost profit, continuing operating expenses and extra expenses the insured incurs while being shut down due to a hacking event (ransomware, malicious code, denial of service attack)
- [ ] **Business Interruption System Failure**: coverage for lost profit, continuing operating expenses and extra expenses the insured incurs while being shut down due to an unplanned outage (human or operational error, coding error)
  Business Interruption Waiting Period: the period of time that must elapse before business interruption coverage is effective
- [ ] **Dependent Business Interruption System Failure**: Dependent Business Interruption Security Failure – coverage for lost profit, continuing operating expenses and extra expenses the insured incurs while being shut down due to an unplanned outage (human or operational error, coding error) at a 3rd party that provides them services under a written contract
- [ ] **Dependent Business Interruption Security Failure**: coverage for lost profit, continuing operating expenses and extra expenses the insured incurs while being shut down due to a hacking event (ransomware, malicious code, denial of service attack) at a 3rd party that provides services under a written contract
- [ ] **Dependent Business Interruption Vendor Type**: The type of vendors that dependent business interruption extends to:
  IT Providers Only - only those vendors that provide the insured an IT service under written contract.
  IT & BPO - only those vendors that provide the insured an IT service or business process outsource service under written contract.
  All contracted providers - all vendors that have a written contract with the insured other than ISPs, utilities and security exchanges
- [ ] **Dependent Business Interruption Waiting Period**: the period of time that must elapse before dependent business interruption coverage is effective
- [ ] **Indemnity Period**: the maximum length of time available to an insured to suffer a business interruption claim from the first outage. The time period can be reduced by a restoration of the network or a return to operations.
- [ ] **Data Restoration**: coverage to recover or restore data lost in a security failure or privacy event
- [ ] **Bricking**: coverage for the replacement of hardware as a result of a security failure that renders the hardware useless
- [ ] **Reputational Harm**: coverage for loss of future customers due to a cyber incident negatively affecting the insured's business
- [ ] **Voluntary Shutdown**: coverage triggering the business interruption portion of the policy when an insured has to voluntarily pull their network offline to prevent an attack
- [ ] **Proof of Loss**: coverage for the insured to engage a 3rd party to help them create proof of loss during the claim process