

Covers first-party cyber and privacy liability for any business. Companies that sell software, IT, or technology services also complete CWCO-SUP-TECHEO for Technology E&O. Complete with CWCO-SUP-CORE and ACORD 125. Answer every question; mark N/A where a question does not apply. Cyber policies are typically claims-made, and defense costs may reduce the limit.

1 APPLICANT / BUSINESS INFORMATION

LEGAL BUSINESS NAME	DBA	FEIN	YEARS IN BUSINESS
BUSINESS ADDRESS	CITY / STATE / ZIP	WEBSITE	

Entity type:
☐ Sole proprietor ☐ Partnership ☐ LLC ☐ Corporation

PRIMARY CONTACT / TITLE	PHONE	EMAIL
CURRENT ANNUAL REVENUE (\$)	PROJECTED REVENUE — NEXT 12 MONTHS (\$)	ADDITIONAL WEBSITES / DOMAINS

2 DATA & TECHNOLOGY PROFILE

Records containing personal information (including records held by vendors):

☐ Under 250,000
 ☐ 250,001 - 1 million
 ☐ 1 - 5 million
 ☐ 5 - 10 million
 ☐ Over 10 million

2-1 Should any subsidiaries be covered? ☐ Yes ☐ No
 IF YES, EXPLAIN

2-2 Does the applicant collect biometric data (fingerprints, face, voice, retina)? ☐ Yes ☐ No
 IF YES, EXPLAIN

2-3 Does the applicant mine, trade, exchange, or hold cryptocurrency or digital tokens? ☐ Yes ☐ No
 IF YES, EXPLAIN

2-4 Does the applicant host, process, or manage data or IT systems for others? ☐ Yes ☐ No
 IF YES, EXPLAIN

2-5 Does the applicant accept payment cards? ☐ Yes ☐ No
 IF YES, EXPLAIN

2-6 If yes to 2-5, is the applicant (or its payment processor) PCI-DSS compliant? ☐ Yes ☐ No
 IF NO, EXPLAIN

3 EXPOSURE & RISK QUESTIONS — PAYMENT FRAUD, RANSOMWARE & ACCESS CONTROLS

The FBI's 2025 report counted \$3.05 billion in business email compromise losses — the costliest cybercrime businesses routinely face — and 3,611 ransomware complaints, whose \$32 million in reported losses excludes the far larger cost of downtime. Payment verification, MFA, endpoint detection, and backups that survive an attack are the controls carriers require.

3-1 Is every payment or wire request verified by phone (using a known number) before funds are sent? ☐ Yes ☐ No
 IF NO, EXPLAIN

3-2 Are changes to vendor or customer bank details verified out-of-band before they take effect? ☐ Yes ☐ No
 IF NO, EXPLAIN

3-3 Do payments above a set amount require approval by two people? ☐ Yes ☐ No
 IF NO, EXPLAIN

3-4 Is multi-factor authentication required for email, including webmail? ☐ Yes ☐ No
 IF NO, EXPLAIN

3-5 Is multi-factor authentication required for all remote access to the network? ☐ Yes ☐ No
 IF NO, EXPLAIN

3-6 Is multi-factor authentication required for administrator and privileged accounts? ☐ Yes ☐ No
 IF NO, EXPLAIN

Endpoint security in place (check all that apply):

☐ Standard antivirus ☐ Next-gen antivirus ☐ EDR ☐ XDR ☐ Managed detection & response (MDR) ☐ None

ENDPOINT SECURITY VENDOR

MANAGED SECURITY PROVIDER (IF MDR)

3-7 Are backups of critical data made at least weekly? ☐ Yes ☐ No
IF NO, EXPLAIN

3-8 Is at least one backup copy offline, air-gapped, or immutable? ☐ Yes ☐ No
IF NO, EXPLAIN

3-9 Have backups been restored in a test within the last 12 months? ☐ Yes ☐ No
IF NO, EXPLAIN

3-10 Is there a written incident response plan? ☐ Yes ☐ No
IF NO, EXPLAIN

3-11 Do all employees complete phishing and security training at least annually? ☐ Yes ☐ No
IF NO, EXPLAIN

3-12 Does the network run any unsupported (end-of-life) software or operating systems? ☐ Yes ☐ No
IF YES, EXPLAIN

4 NETWORK, EMAIL & VENDOR SECURITY

4-1 Is email filtered, with attachment and link sandboxing? ☐ Yes ☐ No
IF NO, EXPLAIN

4-2 Are all internet access points protected by firewalls? ☐ Yes ☐ No
IF NO, EXPLAIN

4-3 Is access to sensitive data limited to people who need it for their jobs? ☐ Yes ☐ No
IF NO, EXPLAIN

4-4 Is sensitive data encrypted at rest? ☐ Yes ☐ No
IF NO, EXPLAIN

4-5 Is a penetration test performed at least annually? ☐ Yes ☐ No
IF NO, EXPLAIN

4-6 Do vendors with access to the network use multi-factor authentication? ☐ Yes ☐ No
IF NO, EXPLAIN

4-7 Are rights, licenses, and releases obtained before publishing content created by others? ☐ Yes ☐ No
IF NO, EXPLAIN

5 EXPOSURE & RISK QUESTIONS — WEBSITE TRACKING & WRONGFUL COLLECTION

Privacy claims are shifting from breaches to how data is collected. Suits under California's wiretap law (CIPA) target pixels, session replay, and chat tools that fire before a visitor consents, with statutory damages of up to \$5,000 per violation, and some carriers now exclude wrongful collection.

5-1 Does the website or app use third-party tracking pixels, session replay, or chat tools (for example, Meta Pixel or TikTok Pixel)? ☐ Yes ☐ No
IF YES, EXPLAIN

5-2 If yes to 5-1, do those tools wait to load until the visitor gives consent? ☐ Yes ☐ No
IF NO, EXPLAIN

5-3 If yes to 5-1, has the website been checked to confirm tracking stops when a visitor declines? ☐ Yes ☐ No
IF NO, EXPLAIN

5-4 Does the website offer video content to visitors while also using third-party tracking tools? ☐ Yes ☐ No
IF YES, EXPLAIN

5-5 Has the applicant received a demand letter or lawsuit alleging wiretapping or wrongful data collection (CIPA, VPPA, BIPA, or similar)? ☐ Yes ☐ No
IF YES, EXPLAIN

6 INCIDENT & COVERAGE HISTORY

6-1 In the past 3 years, has the applicant had a cyber incident, data breach, or media liability claim? ☐ Yes ☐ No
IF YES, EXPLAIN

6-2 Has any cyber incident cost more than \$10,000 or led to a lawsuit or formal dispute? ☐ Yes ☐ No
IF YES, EXPLAIN

6-3 Has the applicant or a key vendor had an unplanned outage lasting more than 6 hours in the past 3 years? ☐ Yes ☐ No
IF YES, EXPLAIN

6-4 Is anyone proposed for coverage aware of a breach or event that could result in a claim? ☐ Yes ☐ No
IF YES, EXPLAIN

6-5 Has cyber coverage ever been declined, cancelled, or non-renewed? ☐ Yes ☐ No
IF YES, EXPLAIN

CURRENT CYBER CARRIER / LIMIT CERTIFICATIONS (SOC 2, ISO 27001) / IR RETAINER

Limit requested (each claim / aggregate):
☐ \$250K / \$250K ☐ \$500K / \$500K ☐ \$1M / \$1M ☐ \$2M / \$2M ☐ \$3M / \$3M ☐ \$5M / \$5M ☐ Other

7 SIGNATURE & FRAUD WARNING

The undersigned declares that the statements and answers given in this supplemental are true, complete and correct to the best of their knowledge, and that no material fact has been withheld or misstated. The applicant agrees that this supplemental, together with all ACORD applications and attachments, forms the basis of any submission to insurers and may be relied upon by them. Signing this supplemental does not bind coverage. This supplemental is an intake document prepared by Cory Washington & Co. LLC to support carrier submission; it does not itself provide coverage.

FRAUD NOTICE: Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance containing any materially false information, or conceals for the purpose of misleading information concerning any fact material thereto, may be committing a fraudulent insurance act, which is a crime and may subject such person to criminal and civil penalties. State-specific fraud warnings appear on the insurer's application.

APPLICANT / AUTHORIZED SIGNATURE (TYPE FULL NAME)	TITLE	DATE
PRODUCER — CORY WASHINGTON & CO. LLC	PRODUCER SIGNATURE (TYPE FULL NAME)	DATE