ChatGPT

CFC Underwriting — *Technology* v4.1 (Tech E&O & Cyber)

- **Per-Claim Limit / Aggregate:** Set in Declarations; generally one overall "Policy Limit" applies per claim and in the aggregate (carrier offers up to **$10 million** combined tech E&O/cyber limits) [1] . For example, CFC's tech policy can be issued up to a $10 million limit (currency can be USD/GBP/EUR) for all E&O, media, and cyber coverages [1] .
- **Retention (Deductible):** Set per policy; varies by risk. CFC notes a **minimum deductible of $0** (some coverages start with no retention) [1] . In practice, deductibles are typically selected in the **$5k–$50k+** range, with $0 retained on initial incident response costs [2] [1] .
- **Breach Response Costs Sublimit:** Provided via a dedicated "incident response" tower **equal to the full policy limit** (in addition to the main limit) [2] [3] . CFC's cyber coverage includes an separate incident response limit so that all breach response expenses (forensics, notification, crisis PR, etc.) do not erode the primary liability limit [3] . In other words, if you buy (for example) a $1 million policy, you get an additional $1 million solely for incident response costs [3] . This separate IR limit is accessible with **$0 deductible** to encourage prompt reporting [2] .
- **Forensics, Notification, PR Sublimits:** No individual sub-cap; these expenses fall under the incident response limit. The policy's Cyber Incident Response coverage covers **IT forensic investigations, legal guidance for notification, notification fulfillment (including call-center services), credit monitoring, and public relations consultants** as needed [4] . All such breach-response costs draw from the dedicated incident response limit (equal to the policy limit) rather than the liability aggregate [3] .
- **Business Interruption (BI) Sublimit:** No separate sublimit – covered up to the full policy limit (subject to waiting period). Income loss and extra expense from a covered cyber event or system failure are payable up to the policy's limit of liability [5] . Notably, CFC's coverage includes **unlimited reinstatements** for BI losses in the period [5] , meaning multiple incidents can be covered (the policy limit applies per event).
- **Dependent BI Sublimit: No sublimit** – CFC covers dependent/system supplier outages at full policy limits [5] . The policy provides *"full supply chain business interruption"* coverage with no separate cap for losses resulting from outages at cloud providers or IT suppliers [5] . (Many competitors sublimit this exposure, but CFC's form covers dependent BI to the same limit as primary BI [6] [5] .)
- **Regulatory Fines Sublimit:** No special sublimit – covered within the policy limit. CFC's Insuring Clause for Regulatory Investigation Costs covers insurable fines and penalties arising from tech services or cyber events up to the overall policy limit (fines uninsurable by law remain excluded) [7] [5] . In other words, any covered regulatory penalties (e.g. GDPR fines) are payable up to the full limit of liability, as long as insurability criteria are met.
- **PCI-DSS Assessment Sublimit: No fixed sublimit** in wording – included up to full limit (separate coverage section). CFC explicitly covers PCI fines, penalties and card brand assessments under its PCI insuring agreement, without a lower cap [8] . The PCI coverage is subject to the overall policy limit, and CFC commits to providing full policy limits for PCI liabilities (assuming the insured meets PCI compliance requirements) [9] . *Note:* Many insurers restrict PCI coverage, but CFC offers it up to the full limit of liability [9] .

Sources: CFC Technology product brochure (2025) [1] [2] ; CFC incident response article [3] ; MSSP Alert news on BI coverage [5] ; Corvus blog on PCI coverage (notes CFC's full-limit PCI stance) [9] . (CFC specimen

wording confirms that exact amounts for limits, sublimits, and retentions are set in the Declarations) [10] [11].

Corvus (Travelers) — *Smart Tech E&O*® (Tech & Prof. Services Liability Endorsement)

- **Per-Claim Limit / Aggregate:** Chosen in Declarations. Corvus's Smart Tech E&O policies offer limits up to **$5 million** per claim and in the aggregate for primary coverage [12]. Typically the each-claim limit equals the aggregate limit (e.g. a $1M each claim / $1M aggregate policy, or up to $5M each/agg), as is standard in claims-made liability policies [12] [13]. *(Corvus indicates businesses up to $2B revenue can secure up to $5M limits on Travelers paper.)*
- **Retention (Deductible):** Set per policy; varies by insured size and risk. Common retentions range from $10,000 to $50,000+ per claim [14]. Corvus offers a retention reduction incentive: a 25% retention credit (up to $25k reduction) for policyholders who engage in its risk prevention services [15]. For example, an insured with a $20k deductible could see it lowered to $15k by completing certain cybersecurity measures [15]. *(Initial incident consultation may sometimes be provided without erosion of retention, but generally the full retention applies to first-party and liability claims.)*
- **Breach Response Costs Sublimit: No sublimit – full policy limit applies.** Breach response and remediation expenses are covered as first-party costs up to the policy's overall limit of liability [16]. Unlike some competitors, the Smart Tech E&O form does *not* impose a lower cap on incident response; it pays breach response costs (forensics, notification, crisis management, etc.) until the main limit is exhausted [16]. In other words, the same $X million limit that applies to liability also applies to breach response expenses (they are not carved out with a separate lesser limit).
- **Forensics, Notification, PR Sublimits: No separate sublimits.** Costs for IT forensic investigation, notification of individuals, call center support, credit monitoring, and public relations/crisis management are all included under the breach response coverage and share in the full policy limit [16]. The Corvus policy explicitly lists **"breach response and remediation expenses"** as a covered first-party insuring clause without a specified sub-limit [16], meaning these expenses can be claimed up to the policy's limit. *(Corvus emphasizes that it provides broad incident response coverage without sublimits, to distinguish from carriers who might cap, for example, notification costs.)*
- **Business Interruption (BI) Sublimit: No sublimit – full limit available.** Coverage for business interruption loss (due to security breaches or system failures) is provided up to the policy's limit of liability [17]. There is no lower cap on cyber BI; the insured can recover the loss of income and extra expense from a covered outage up to the same overall $ amount of their policy. (Contingent/business dependent interruption is likewise not sub-limited – see below.) Standard waiting period applies (often 8 hours) [18].
- **Dependent BI Sublimit: No sublimit – covered to full limit.** The Smart Tech E&O form includes **contingent business interruption** (loss from service provider outages) with full policy limits [17]. Corvus specifically highlights that it offers *"contingent business interruption with full policy limits"* [17], unlike policies that might only offer a small sublimit for third-party outages [6]. This means an interruption at a cloud provider or other vendor can trigger the same limit (e.g. $1M) as an incident in the insured's own system.
- **Regulatory Fines Sublimit: No sublimit – full limit.** Coverage for regulatory investigations, fines and penalties (e.g. GDPR/CCPA actions) is included up to the policy's limit [19]. The policy's Third-Party coverage section explicitly covers *"regulatory investigations, fines, and penalties"* and does not assign a

separate cap [19]. Thus, insurable regulatory fines can be paid up to the full limit of liability (subject to legal insurability in relevant jurisdictions).

- **PCI-DSS Assessment Sublimit: No sublimit – full limit.** PCI fines and assessments are covered as a named insuring agreement without a reduced limit [19]. Corvus's policy lists *"PCI DSS assessment expenses"* as part of its third-party coverages and, importantly, **provides full policy limit coverage for PCI fines & penalties** (assuming the insured was PCI compliant) [19] [9]. In industry guidance, Corvus notes that many insurers sublimit PCI exposures, but that **Corvus offers PCI fines coverage up to the full limit** as long as compliance requirements are met [9].

Sources: Corvus Smart Tech E&O product overview [20] [19]; Corvus small-business cyber guide [17] [13]; Aragon insurance broker summary (Corvus) [15]; Corvus blog on PCI coverage [9].

Embroker — *Technology E&O / Cyber* (MGA Package Policy)

- **Per-Claim Limit / Aggregate:** Chosen by insured; typically **$1 million** each claim with $1 million aggregate (standard for startups), with options up to higher limits (Embroker advertises up to **$5 million** total for its tech E&O/cyber package) [21] [22]. The policy is claims-made, so the aggregate is the maximum for all claims in the year (equal to the per-claim max, unless a higher aggregate is separately negotiated, which is not typical) [21]. *(For instance, an Embroker policy might carry a $2M per-claim/$2M aggregate limit; Embroker's marketing indicates $5M as a maximum available primary limit.)*
- **Retention (Deductible):** Starts low; **$5,000 minimum** for small firms [21]. Embroker's program is aimed at startups/SMEs, and it quotes retentions as low as $5k per claim (higher retentions can be selected for premium savings). Certain insuring agreements (e.g. breach response services) may effectively have no deductible or a separate retention structure in some cases (for instance, initial legal consultation might be payable with no retention), but generally each claim will carry the retention listed on the declarations [21] [23]. *(Embroker's sell-sheet notes a $0 deductible option for select accounts, but $5k is the usual floor.)*
- **Breach Response Costs Sublimit: No separate sublimit – full limit applies.** Embroker's policy provides comprehensive breach response coverage (legal, IT forensics, notification, credit monitoring, crisis PR, etc.) as part of the base coverage, up to the policy's full limit of liability [24]. The Embroker Tech E&O/Cyber sell-sheet explicitly shows key first-party coverages (system damage, cyber extortion, business interruption, etc.) all with "Full Policy Limit" — meaning breach response costs are not capped below the overall policy limit [24]. In practical terms, if the policy has a $1M limit, up to $1M can be spent on covered incident response expenses.
- **Forensics, Notification, PR Sublimits: None.** Expenses for forensic investigators, notification services, call centers, credit/ID monitoring, and public relations/crisis management are included in the Breach Response coverage and share the same full policy limit [24]. There are no smaller internal caps for these categories; Embroker's package covers them as needed until the overall limit is reached. (The marketing highlights "breach response costs" generically, which encompass all such expenses with no mention of sublimits [25] [24].)
- **Business Interruption (BI) Sublimit: None – full limit.** Coverage for first-party income loss and extra expense due to network interruption is provided up to the full policy limit [26]. The Embroker coverage sheet lists "Business Income" as Full Policy Limit and does not impose a sublimit on cyber BI [26]. A standard waiting period (e.g. 8 hours) applies, but once triggered, the loss is covered until limits exhaust.

- **Dependent BI Sublimit: None – full limit.** Dependent (contingent) BI from a supplier's outage is also covered up to the policy limit [26]. The policy explicitly includes "Dependent Business Income" with the same Full Policy Limit in the coverage summary [27]. This means losses from third-party cloud or service-provider downtime are indemnified up to the full limit, making the coverage broad (no reduced sublimit for contingent BI).
- **Regulatory Fines Sublimit: None – full limit.** Regulatory defense costs and fines (e.g. arising from privacy regulations) are covered to the full policy limit as part of third-party liability coverage [24]. There is no special cap for regulatory penalties; if a regulatory action (like a GDPR fine) is covered, the policy will pay up to the same overall limit of liability (subject to legal insurability of the fine).
- **PCI-DSS Assessment Sublimit: None – full limit.** PCI fines, penalties, and card network assessments are included as a covered loss up to the full policy limit [28]. Embroker's schedule shows "PCI Fines, Assessments or Charges: Full Policy Limit" [28], indicating no separate lower cap. (The policy likely requires PCI compliance; if the insured is non-compliant at the time of breach, coverage may be affected, but there is no built-in dollar sublimit for PCI— it shares the main limit.)

Sources: Embroker Tech E&O/Cyber sell-sheet (2024) [21] [24]; Embroker marketing overview [25]. *(Embroker's public-facing materials are high-level; the internal coverage sheet confirms all primary coverages use the full policy limit, with only certain crime add-ons having fixed sublimits [29].)*

Beazley — *MediaTech* (Tech E&O + Media + Cyber, Form F00731 02/2019)

- **Per-Claim Limit / Aggregate:** Set in Declarations. Beazley's MediaTech is typically offered with combined single limits up to **$5 million** for SME accounts [30] (higher limits, e.g. $10M–$25M, are available for larger risks [31]). The policy aggregate equals the per-claim maximum in most cases (e.g. a $3M each claim / $3M aggregate). MediaTech is a **"defense within limits"** claims-made form, so the stated limit is the max for all defense + indemnity across all claims [32] [33]. *(Example: An insured might carry a $2M aggregate – any one claim can consume up to $2M, and all claims together cannot exceed $2M.)*
- **Retention (Deductible):** Set per coverage part in Declarations; varies by insured size/risk. Common retentions for MediaTech range from **$10,000** to **$50,000** each claim (could be higher for larger limits). Notably, **breach response services often carry a low retention or none**: Beazley's Breach Response coverage can be structured with per-incident retentions as low as $5k (and even a $0 deductible option for certain expenses like initial legal consultation) [23]. For instance, legal and forensic expenses to triage a breach may trigger only a $5k retention, even if the main policy E&O retention is higher [23].
- **Breach Response Costs Sublimit: Separate dedicated limit (outside liability limit).** MediaTech includes Beazley's signature Breach Response coverage with its own aggregate limit for incident response costs. By default this **"Breach Response" limit is often set at $****1 million to $2.5 million** and does **not erode** the policy's main liability limit [34]. For example, Beazley's BBR program provides up to $2.5M for breach response expenses (legal, IT forensics, notification, credit monitoring, PR) and covers up to 5 million individuals notified, separate from the indemnity limit [34] [35]. MediaTech typically follows this model: the Declarations specify a Breach Response sublimit (which can be equal to or less than the policy aggregate). All breach response costs are paid out of this sublimit, leaving the full main limit available for liability claims [36] [37]. *(Beazley's small-business MediaTech brochure emphasizes "breach response services (where available)" and indicates limits up to*

$5M for the package [31] [38]. In practice, the breach response sub-limit is tailored to the insured's needs – it can be as high as the full policy limit, though many choose a sublimit in the $100k–$1M range for cost reasons.)

- **Forensics, Notification, PR Sublimits: Covered under Breach Response limit.** The Breach Response insuring agreement covers the full suite of incident response costs: **legal counsel, computer forensic investigators (including PCI forensic investigators), notification services, call-center support, credit/identity monitoring, and public relations/crisis management** expenses [39] [40]. These individual elements do **not** have separate caps; they draw from the overall Breach Response sublimit. For example, if the Breach Response limit is $1M, that $1M can be used as needed for any combination of legal, IT, notification, PR, etc., over an 18-month period following a breach [41]. (Beazley's policy specifies that credit monitoring is provided for up to 5 million individuals under the breach response limit, indicating how generous that separate limit can be [35].)
- **Business Interruption (BI) Sublimit: No built-in sublimit (uses policy limit).** First-party *Business Interruption Loss* coverage (from security breaches or system failures) is available up to the full policy limit, unless the insured chooses a lower sub-limit in the schedule [42]. By default, the BI coverage limit equals the Policy Aggregate. The specimen wording does not impose a smaller cap, and the product facts indicate full limits for cyber BI (e.g. "business interruption loss from security breach or system failure" is a core coverage) [42]. Waiting period is specified in Declarations (often 8–12 hours) [43].
- **Dependent BI Sublimit: Included within BI limit** (not a separate additional limit). The policy covers *Dependent Business Interruption* (loss from a vendor or cloud provider breach) as an extension of the BI coverage [44] [45]. There is **no separate standalone limit** for dependent BI – any dependent BI loss will use the same BI insurance limit. In the wording, the Dependent BI coverage is explicitly *"part of"* the BI limit [46]. This means if the BI/Dependent BI limit is $1M combined, a loss due to a third-party outage can be paid up to $1M but would exhaust the same $1M aggregate available for the insured's own BI losses. *(Also note: pure utility/Internet infrastructure failures not caused by a cyber event are excluded, so Dependent BI only applies if the vendor's downtime is due to a security breach or system failure)* [47].
- **Regulatory Fines Sublimit: No separate sublimit** – covered to full limit. The *Regulatory Defense and Penalties* insuring agreement provides coverage for regulatory investigations, fines and penalties arising from data or security breaches, up to the policy's liability limit [48]. There is no smaller cap unless one is scheduled. Beazley's form defines "Penalties" broadly and covers them where insurable by law [49]. Thus, if the policy aggregate is $5M, up to $5M could be used for regulatory fines/defense (subject to legal insurability in the venue).
- **PCI-DSS Sublimit: Yes – typically sublimited.** Payment Card Liabilities & Costs (PCI contractual assessments) are covered under a dedicated insuring clause, often with a modest sublimit (e.g. **$100,000** or another amount selected). The specimen policy provides a PCI coverage section [50], but the actual dollar limit for PCI fines is set in the Declarations. In many cases, insurers and insureds agree to a sublimit for PCI (e.g. 100k–500k) given the unpredictability of card brand assessments. The Beazley Breach Response program, for instance, offers a *"separate sublimit of coverage for fines and penalties resulting from PCI-DSS noncompliance"* [51]. MediaTech policies generally include PCI coverage but **with its own sublimit that is part of (not in addition to) the aggregate** [51]. For example, an insured might have a $1M policy with a $250k PCI fines sublimit – any PCI fines would be paid up to $250k, and that amount also reduces the overall $1M aggregate. *(PCI forensic investigation costs, however, are covered under Breach Response costs and not subject to the PCI sublimit)* [51] [52].

Sources: Beazley MediaTech small business summary [30] [40]; Beazley BBR coverage fact sheet [34] [51]; MediaTech specimen form analysis [53] [46]; Beazley brochure (Oct 2022) [31].

AXA XL — *CyberRiskConnect* (Privacy, Security & Tech Insurance, Form TRD 050 0619)

- **Per-Claim Limit / Aggregate:** Flexible; can be written with a **Combined Aggregate Limit** for all coverages or Separate Aggregates for certain coverages [54] [55]. In a typical configuration, the policy has a single Combined Aggregate (e.g. **$5 million** for all claims in the period) which also functions as the per-claim cap (since no claim can exceed the aggregate). For example, one public entity policy shows a **$6 million each claim** and **$6 million policy aggregate** limit on CyberRiskConnect [56] [57]. AXA XL's capacity is high; large organizations can obtain limits in the tens of millions (e.g. $10M, $25M+), though standard buyers carry $1M–$5M. The insured may elect a "Separate Limits" option where first-party coverages have one aggregate and certain coverages (like breach response) have another, but the sum total is still capped (see Breach Response below) [54] [58].
- **Retention (Deductible):** Varies; set individually for each insuring agreement in the Declarations. Typically, third-party liability sections and first-party sections each carry a retention that can range from **$10,000** for small accounts to **$50k–$100k** (or more) for larger risks. AXA XL allows different retentions by coverage (e.g. one could choose a higher retention on E&O claims but a lower one on breach response costs). For instance, a policy might have a $25k retention for liability claims, $10k for business interruption, and $0 for certain crisis management expenses. *Source:* (The specimen form notes retention applies to each coverage part as listed in Item 4 of Dec; public-sector pools have used retentions like $100k on liability [59]. AXA XL also sometimes offers a co-insurance or waiting period in lieu of large retentions on BI cover.)
- **Breach Response Costs Sublimit: Available as a separate aggregate limit** (if Separate Limits option chosen). CyberRiskConnect's *Data Breach Response & Crisis Management* coverage can be structured so that it has its own dedicated aggregate apart from the liability limit [60]. Under the "Separate Limits" configuration, the policy will specify a *Data Breach Response Aggregate Limit* (for example, $1M solely for breach response costs) which is the max the insurer will pay for all incident response expenses [60]. This breach response limit does **not erode** the Third/First-Party Aggregate in that setup [55] [58]. If the insured instead elects Combined Limits, then breach response costs share in the one combined policy limit (and a sublimit for breach response can still be stated if desired, capping that coverage) [61] [62]. In summary: the client can either have breach response inside the main aggregate (possibly with a sublimit) or carve it out with its own bucket. Many policyholders choose a separate bucket so that, say, $500k for breach costs won't deplete their $5M liability cover.
- **Forensics, Notification, PR Sublimits: Covered under Breach Response coverage (no individual caps).** The Data Breach Response & Crisis Management insuring clause covers all reasonable breach response expenses for up to 18 months following a breach [41]. This includes legal breach coaching, IT forensic investigations (including *PCI Forensic Investigator* fees) [52], notification and credit monitoring for affected individuals, call center services, and public relations/crisis management costs. There are no separate dollar sublimits per expense type in the policy form – all such costs accumulate toward the overall breach response limit or the combined policy limit, depending on the structure [63] [58]. For example, if $100k is spent on forensics and $50k on PR, that $150k counts against the breach response aggregate. The only constraints are time (costs must be incurred within 18 months of the breach) and the overall breach response limit chosen.

- **Business Interruption (BI) Sublimit: No inherent sublimit – usually full policy limit.** The *Business Interruption & Extra Expense* coverage (Insuring I.B.1) pays loss of income due to a cyber security breach-induced outage, typically up to the policy's aggregate limit (unless a distinct sublimit is listed) [64]. In the standard configuration (Combined Limits), there is no separate BI cap: the insured could potentially use the entire policy limit for a major business interruption loss. In practice, some insureds opt to set a specific sublimit for BI (for instance, they might only want $2M of their $5M policy to apply to BI), which would be noted in the schedule. But if not specified, BI can exhaust the full limit. *(AXA XL does exclude purely external infrastructure failures [65], so the BI must result from a breach or security incident, not a general power outage.)* Waiting Period is typically listed (commonly 8 or 12 hours).
- **Dependent BI Sublimit: Not covered by default.** The base CyberRiskConnect form does *not* include coverage for dependent system outages unless endorsed. In fact, the policy's exclusions make clear that outages of utilities/Internet not under the insured's control are excluded unless they result from a covered cyber attack on that infrastructure (and no affirmative contingent BI insuring clause is present) [65]. Unlike some cyber policies, standard AXA XL CyberRiskConnect does **not provide Dependent Business Interruption coverage out of the box** – loss from a third-party provider's failure would generally be excluded as "Infrastructure Failure" unless specifically negotiated back. Therefore, there is effectively **no Dependent BI sublimit** because the exposure is not covered (except via custom endorsement or if the third-party outage is caused by a defined cyber event).
- **Regulatory Fines Sublimit: No sublimit – full limit applies.** The policy's *Privacy Regulatory Defense, Awards & Fines* insuring agreement (I.A.5) covers civil penalties and regulatory damages resulting from privacy/security violations, up to the policy's liability limit [66]. There isn't a smaller cap unless the insured opts for one. Thus, if an insured carries $5M limit, a covered regulatory fine (e.g. for a data breach) could be paid up to $5M (provided such fines are insurable; the form defers to most-favorable-law on insurability of fines) [49].
- **PCI-DSS Assessment Sublimit: Not covered (no standard PCI coverage).** The off-the-shelf CyberRiskConnect form does **not include PCI fines/assessments** as an insured loss category. PCI obligations would typically fall under contractual liability, which is excluded (no insuring clause covers them) – and there is no built-in carve-out for PCI assessments [67]. In other words, unless an endorsement is added, **PCI fines and card brand assessments are not covered** by the policy. (The policy *does* cover the cost of a mandated PCI Forensic Investigator in the event of a breach – that is considered a breach response cost [52] – but any resulting PCI fine or penalty from the card networks is not covered.) Many insureds facing PCI exposure must request an endorsement to add a sublimit (often $100k) for PCI fines. If such an endorsement is in place, that sublimit would apply (commonly $100k–$250k). Absent that, PCI assessments are effectively self-insured.

Sources: AXA XL CyberRiskConnect policy form [54] [58]; Camden Co. coverage schedule example [57]; AXA XL policy excerpt on limits options [61] [63]; Exclusion for infrastructure failure (no dependent BI) [65]; Privacy regulatory insuring clause [66]; Beazley report (notes many policies exclude or sublimit PCI) [68] and AXA XL press (sublimits introduced for certain exposures) [69]. (The CyberRiskConnect specimen confirms the insured may choose combined vs separate limits and that sublimits, if any, are stated in the Declarations for each insuring agreement) [63] [55].

---

[1] webcdn.cfc.com
https://webcdn.cfc.com/media/4okafsv0/technology_product-brochure_row_2025.pdf

2 webcdn.cfc.com
https://webcdn.cfc.com/media/jxlo0ddh/technology_product-brochure_au_0525_v2.pdf

3 Cyber coverage: Nil deductible and separate limit for incident response costs | CFC
https://www.cfc.com/en-au/knowledge/resources/articles/2024/08/cyber-coverage-highlights-nil-deductible-and-separate-limit-for-incident-response/

4 7 8 10 11 0_00_corgi.md
file://file-4u8VNE2EynpozEJ3dkf9CG

5 Cyber Insurance Provider CFC Unveils Business Interruption Coverage - | MSSP Alert
https://www.msspalert.com/news/cfc-cyber-insurance-coverage

6 2025Q1 Tech E&O Guide for MSPs — Beltex Insurance
https://www.beltexins.com/insights/2025q1-tech-eampo-guide-for-msps

9 68 What Are PCI Fines and Penalties?
https://www.corvusinsurance.com/blog/cyber-coverage-explained-pci-fines-and-penalties-coverage

12 16 19 20 Smart Tech E&O® Insurance Coverage from Corvus by Travelers
https://www.corvusinsurance.com/smart-tech-e-o-and-excess

13 15 17 Corvus Cyber Insurance | Documents | Aragon Way Insurance
https://aragonway.com/cyber-insurance/corvus/corvus-documents/

14 2024 / 2025 Tech E&O Guide for MSPs - Beltex Insurance
https://www.beltexins.com/msp-techeo-2024

18 21 24 26 27 28 29 Access_Tech EO/Cyber_Sell Sheet_May 2024
https://access.embroker.com/wp-content/uploads/2024/06/Access_Tech-EO_Cyber_Sell-Sheet_May-2024.pdf

22 [PDF] Excess Sell Sheet 4 (Mshift Only)
https://20454591.fs1.hubspotusercontent-na1.net/hubfs/20454591/Excess%20Sell%20Sheet%204%20(Mshift%20Only).pdf

23 34 35 36 37 51 beazley.com
https://www.beazley.com/globalassets/cyber/documents/brochures/beazley-bbr-coverage-factsheet-us.pdf

25 2_10_embroker.md
file://file-HW7uXSCw2s13ooTpB9EXq7

30 38 40 42 MediaTech for Small Businesses | beazley
https://www.beazley.com/en-US/products/small-business-solutions-usa/mediatech-for-small-businesses

31 MediaTech - Beazley
https://beazley.com/en-001/products/cyber-london-market/mediatech/

32 33 39 43 44 45 46 47 48 49 50 53 3_04_beazley.md
file://file-DrJdpTJKZS9yDvtiYZK42f

41 52 54 55 58 60 61 62 63 CyberRiskConnect Privacy, Security and Technology Insurance
https://axaxl.com/-/media/axaxl/files/pdfs/insurance/cyber-north-america/cyberriskconnectpolicyform_axaxl_trd-050-0619.pdf?rev=6dd3432507d145559285773ddf4468f2&sc_lang=pt&hash=BB75873199AFFE20F7C8DCCC79C25BD3

56 [PDF] CYBER LIABILITY INSURANCE OVERVIEW
https://des.wa.gov/sites/default/files/2025-02/APIP-Cyber-Liability-Insurance-Overview.pdf

57 XL Indian Harbor Cyber Members of the Camden County Mun.pdf
https://opramachine.com/request/9299/response/17213/attach/html/4/XL%20Indian%20Harbor%20Cyber%20Members%20of%20the%20Camden%20County%20Mun.pdf.html

59 [PDF] MISSOURI UNITED SCHOOL INSURANCE COUNCIL 2020 PLAN ...
https://www.musicprogram.org/wp-content/uploads/2020/03/2020-MUSIC-Plan-Document-With-Attachments.pdf

64 65 66 67 4_02_axa.md
file://file-KFgt22wHWgSesDSHDizgcR

69 [PDF] CyberRiskConnect Product Overview - AXA XL
https://axaxl.com/-/media/axaxl/files/pdfs/insurance/cyber-north-america/cyber-and-tech-product-sheet_axa-xl_us.pdf