

E-Business (“Cyber”) Liability Insurance “Quick” Checklist

Aspect	Notes/Comments
1. What is the policy coverage territory? (At a minimum, it should be “worldwide” – even better would be “universal” or “anywhere”.)	
2. The policy should provide for an affirmative coverage statement for punitive damages (“most favorable jurisdiction” language would be a plus).	
3. Does the policy address errors and omissions coverage? To what extent? (This will vary greatly from policy to policy.) Is all E&O covered, or just E&O pertaining to specific functions/systems?	
4. Does the coverage apply to insureds’ networks (and systems) or is it less in coverage scope (broader is better, but also more expensive)?	
5. It is important to have specific coverage for “...invasion of privacy/breach of confidentiality...”, or some generally equivalent wording. Language which covers unauthorized use/disclosure of All Private Information is in the best coverage forms.	
6. It is important to have specific coverage for allegations of “...breach of security...” or “...failure of security to prevent unauthorized access...”, or some generally equivalent wording.	
7. It is important to have specific coverage for allegations of “...unauthorized access...” – and related claims. (This may or may not be included within important coverage provisions for “...breach of security...”.)	
8. Does the policy provide at least some coverage for employee theft or employee dishonesty coverage? (This is important because traditional “crime” insurance will almost certainly <u>not</u> cover losses involving <u>intangible</u> property; however, DIRECT COVERAGE for employee dishonesty is difficult to find.) At least we should request “final adjudication” wording for any employee dishonesty – related exclusionary language.	
9. Is there automatic coverage for newly acquired organizations? Generally there will be some coverage, usually limiting the size of entities automatically covered to some percentage of the consolidated asset size of the acquiring entity.	

	Aspect	Notes/Comments
10.	How does this policy provide coverage for intellectual property? (It should be broad enough to cover <u>at least</u> copyright and trademark infringement – don't expect coverage for any form of patent infringement, and maybe not even "trade secrets".)	
11.	It is important to make sure that all subsidiaries are covered under the policy definition of subsidiary.	
12.	It is important <u>not</u> to have exclusionary language for "... failure to obtain/maintain insurance ..."	
13.	It is important <u>not</u> to have exclusionary language for "... failure of security of a [subject] computer system ..."	
14.	Is there coverage for theft of a laptop, PDA, server or other computer equipment? This is a frequent occurrence and we should strive for this coverage if at all possible.	
15.	We need to understand the extent to which source code is covered or excluded. It may not be important to a consultant, or even to a small financial institution, but it is critically important if there is a software or hardware design exposure.	
16.	Is there coverage for reimbursement of notification costs in the event of a Security Breach? (Most states mandate that their residents be notified in the event of a data security breach, and under the Federal HI-TECH legislation - within the Stimulus Legislation of early 2009- it is mandated that employers must formally notify employees in the event of a data breach involving employee health records, so having insurance proceeds to address this exposure is VERY desirable.) [Coverage for this exposure is known by various names: Public Relations Expense; Privacy Breach Expenses; Crises Management Expenses, etc.]	
17.	It is of some importance that the insured's consent be required prior to settling claims. Almost all e-business coverage forms are written on a "duty to defend" basis.	
18.	Does the liability coverage apply "enterprise-wide" (to ALL operations), or just to electronic operations of the organization? Although not routine, many cyber liability insurance products will at least offer, for an additional premium, coverage applicable on an "enterprise" basis, which would pick up both real as well as virtual, exposures.	

Aspect		Notes/Comments
19.	Does the liability coverage provided afford full defense and indemnity coverage for regulator-brought litigation?	
20.	It is important (for most insureds) to have no policy exclusion for payment card industry standards (affirmative coverage for this exposure would be better, but is likely unavailable).	
21.	It would be desirable NOT to have policy exclusions for privacy claims relating to collection of information using cookies, bugs, beacons, key-stroke loggers or similar techniques.	
22.	Is there any limitation on the type of media covered? We'd want to see coverage for media claims involving iPods, iPads, PDAs, and even cell phones, as well as USB Flash Drives.	
23.	As respects Content Injury coverage, this should be broad enough to essentially cover any information published in any computer readable format.	

March, 2010 Revision