

Our computer firewalls and virus protections are up to date...

As design professionals your business depends greatly on technology for creating, sharing and communicating with internal and external parties. Some of the most sophisticated technology firms in the world have been faced with a Cyber attack. The technology your company relies upon to conduct its business also makes your firm vulnerable to Cyber attacks that can result in out-of-pocket and reputational costs that can be surprisingly expensive.

What types of Cyber Risks exist for a design professional firm?

When a Cyber Attack occurs there are two potential victims from a breach: (1) confidential information of the design firm's client is exposed (third party loss exposure) and (2) the financial impacts to the design firm, including loss of information, physical damage & business interruption, that did not prevent the security breach (first-party loss exposures). Refer to the "Cyber Risk for A&E firm" for more detailed information on claim scenarios, damages, and insurance coverages.

Our standard insurance policies cover losses from Cyber Risk attacks, don't they?

Many design firms believe that their insurance policies will cover damages to their firm and to third parties from losses due to a Cyber attack. Unless your firm has a stand-alone Cyber Security Liability Policy in place, coverage gaps often exist in most standard policies even when cyber coverages are expressly covered. For example;

- A General Liability insurance policy typically contains Cyber Risk coverage for certain perils and also Exclusions for;
 - Mental Anguish & Humiliation
 - Electronic Data, Intellectual Property, & Blogs

Efforts are underway by the insurance industry (ISO) to introduce a "Security Breach Exclusion" in standard general liability policies which will result in securing a separate Cyber Security Liability Policy in order to cover this exposure.

- A Business Owners Policy often covers first party property damage from losses due to cyber attacks on electronic equipment owned/leased by the design professional but coverage is typically limited to a certain dollar amount or sometimes no coverage is afforded at all unless Electronic Data & Media coverage is endorsed to the policy.
- Some Design Professional Liability insurance policies afford coverage for Network and Information Security Offenses that typically exclude;
 - First party property loss coverage – Your firm's computers, software, laptops, cell phones, etc.
 - Business Interruption – Your firm's loss of profits & continuation of ordinary operating expenses including payroll when unable to operate due to Cyber attack.
 - Computer Program & Electronic Data Restoration – Your firm's costs for repair and restoration of computer programs and electronic data.
 - If coverage applies, claims paid under the policy are subject to a higher deductible than a deductible of a Cyber Security Liability Policy.

What insurance policy is recommended to insure for Cyber attacks and how much will it cost?

Hall & Company's proprietary Cyber Security Liability Policy is designed to cover Cyber attack exposures of a design professional firm;

- First party protection for the design firm, with Loss of Digital Assets, Non-Physical Business Interruption, Extra Expense, Cyber Extortion, Cyber Terrorism, and Security Event Crisis coverage.
- Third party protection for the design firm's clients, with Network Security and Privacy Liability, Employee Privacy Liability, and electronic Media Liability coverage.
- Deductibles as low as \$1,000
- Premiums start as low as \$500 annually.

CLAIM SENARIO	RESULTING COSTS	APPLICATION INSURANCE COVERAGE DESCRIPTION	POLICIES THAT MAY AFFORD COVERAGE		
			BUSINESS OWNERS	A&E PROFESSIONAL LIABILITY	CYBER SECURITY LIABILITY
The insured is sued by a large group of parties as a result of a hacker successfully accessing the insured's telephone system and for a phishing scam where huge phone bills were incurred by the hacker, identify theft occurred and the scammer passed themselves off as the insured to defraud others.	Damages and defense costs for covered lawsuits.	Network and Information Security Liability	?	?	Yes
A lawsuit is brought against the insured alleging defamation and privacy breach from an employee's spontaneous conversation on social media about a competitor.	Costs for responding to regulatory claims stemming from the data breach.	Communications and Media Liability	?	?	Yes
A major data breach occurs that may involve hundreds of clients. Multiple states bring regulatory action against the insured requiring by law notification to their clients of a breach and the potential loss of confidence that clients and prospective clients have placed in your firm.	Costs for hiring a public relations firm to restore confidence or mitigate negative publicity generated from the incident.	Regulatory Defense Expenses	?	?	Yes
The insured's Chief Financial Officer has his laptop stolen while traveling. The laptop contains client records, including confidential property records and their personal contact information.	Costs for hiring a public relations firm to restore donor confidence or mitigate negative publicity generated from the incident.	Crisis Management Event Expenses	?	?	Yes
A disgruntled employee decided to change all administrator passwords to the computer systems which locked the entire company out of their systems. Repairing the problem required a \$500,000 IT security consultants bill to regain company access to its systems and data.	Costs for hiring a breach response firm to find and fix the breach, assist with notice requirements and expenses, provide credit monitoring and a call center for impacted individuals, and obtaining an ID Fraud policy for affected victims.	Security Breach Remediation and Notification Expense	?	?	Yes
A computer virus totally destroys the insured's operating system software and data.	Costs for repair and restoration of the insured's computer programs and electronic data.	Computer Program and Electronic Data Restoration Expenses	?	?	Yes
Unauthorized access is gained by a hacker to the insured's accounts payable in their computer system and alters the bank routing information on outgoing payments, resulting in hundreds of thousands of dollars transferred to third party bank accounts.	Direct loss of the insured's money, securities or other property.	Computer Fraud	?	?	Yes
An insured receives an email that appeared to be from a trusted source but was not. The insured's employee opened the email, which activated a computer virus that tracks key strokes from their computer. The hacker used this tool to obtain password information and make a fraudulent electronic wire transfer from the insured's bank account.	The insured's funds that were fraudulently transferred from its bank account.	Funds Transfer Fraud	?	?	Yes
The insured receives a series of threats of extortion that their computers will be hacked to obtain into confidential data and disclose it to the third parties.	Money or securities paid to the extortioner.	E-Commerce Extortion	?	?	Yes
An insured's computer system crashes due to a virus or hacking and the system is offline for an extended period of time while systems are restored. Damages include lost profits and continued operating expenses including ordinary payroll in order to retain employees.	The net proceeds that would have been earned (or net losses that would have been avoided) resulting from the computer system disruption.	Business Interruption and Additional Expense	?	?	Yes