Published on *The National Law Review* https://natlawreview.com

Cyber-Attacks Against Government Contractors and the Availability of Insurance Coverage

Article By:

Insurance Recovery at Gilbert LLP

Based on recent cyber-attacks against the United States Office of Personnel Management (OPM) and its subcontractors, USIS and KeyPoint Government Solutions, it is evident that government entities and government contractors are prime targets for cyber-attacks given their possession of highly sensitive information. While government contractors should take steps to ensure that their IT systems comply with the terms of their contracts and various other executive orders and standards, equally important, government contractors should take steps to ensure that, in the event of a cyber-security breach, they have maximized their financial protection. Several avenues exist to do so, including the ***Support Anti-Terrorism by Fostering Effective Technology (SAFETY)*** Act of 2002, insurance coverage, and indemnities. This article focuses on potential insurance coverage for cyber-security breaches, and how recent decisions have affected the availability of insurance coverage.

Recent Decisions Regarding Coverage For Cyber-Security Breaches Under CGL Policies

Many companies have relied upon and still rely upon their commercial general liability (CGL) policies to provide coverage for cyber-security breaches. There is mixed authority regarding whether coverage for cyber-security breaches is available under CGL policies, and many jurisdictions have not evaluated this type of coverage under CGL policies.

Several courts have provided coverage for cyber-security breaches under CGL policies. S*ee, e.g.*, *Hartford Cas. Ins. Co. v. Corcino & Assocs.*, 2013 WL 5687527 (C.D. Cal. Oct. 7, 2013); *Retail Ventures, Inc. v. National Union Fire Ins. Co.*, 691 F.3d 821 (6th Cir. Aug. 23, 2012); *Eyeblaster, Inc. v. Fed. Ins. Co.*, 613 F.3d 797 (8th Cir. 2010). Recent decisions, however, potentially limit the availability of coverage for a cyber-security breach under CGL policies. *Zurich Am. Ins. V. Sony Corp. of Am.*, Case No. 651982/2011, 2014 WL 3253541 (N.Y. Sup. Feb. 24, 2014); *Recall Total Information Mgmt. v. Federal Ins. Co.*, 317 Conn. 46, 51-52 (2015).

Insurers are likely to rely on these recent, negative decisions in denying coverage for cyber-security breaches under CGL policies, but government contractors should not accept this coverage determination. Given the conflicting case law and the fact that many jurisdictions have not addressed this issue, there is still the potential for coverage under CGL policies for cyber-security breaches.

Cyber-Security Insurance Policies and Exclusions of Which Government Contractors Should be Especially Wary

In light of these decisions, however, government contractors should evaluate whether to purchase cyber-security insurance coverage. These are specialized insurance policies that specifically provide coverage for cyber-security breaches.

When purchasing this type of policy, government contractors should be aware that these policies are highly negotiable and can be tailored to a government contractor's needs; there is no "form" policy used by insurers. Significantly, in negotiating these policies, government contractors should resist the inclusion of "boilerplate" exclusions, and should be especially wary of the inclusion of an Act of War and Terrorism Exclusion and a "Best Practices" Exclusion (also known as "Minimum Required Practices").

An Act of War and Terrorism Exclusion typically excludes coverage for state-sponsored acts of war or terrorism. Because government contractors are in the unique position of holding sensitive information for federal and state agencies, government contractors are prime targets for state-sponsored cyber-attacks, and potentially may implicate this exclusion.

The "Best Practices" Exclusion typically excludes coverage where an insured fails to implement the procedures and risk controls that are set forth in its application. In a recently-filed case in California, an insurer is invoking this exclusion to avoid its coverage obligations for a cyber-security breach, contending that the insured did not utilize appropriate encryption and other security measures. *Columbia Casualty Co. v. Cottage Health Systems*, No. 2:15-cv-03432 (C.D. Cal). This decision will provide significant insight regarding an insured's obligations with regard to security measures, given the ever-evolving landscape of cyber-security threats and security measures.

Because government contractors are subject to a patchwork of federal and state orders, laws, and regulations, and agency specific requirements regarding appropriate electronic security measures, what constitutes "best practices" for a government contractor is a complex web that may provide an insurer an avenue to avoid coverage. Government contractors should push to delete the "Best Practices" Exclusion from their cyber-security policies, but at a minimum, should make clear the benchmark that needs to be met to satisfy "best practices."

Conclusion

Given the evolving landscape of insurance coverage for cyber-security breaches, government contractors must not only act proactively to ensure that their insurance portfolios provide sufficient coverage, but should also be prepared if a cyber-security breach occurs by setting forth the process they will enact to combat both the reputational and financial harm caused by such a breach. When a breach occurs, government contractors should coordinate with coverage counsel to review their policies, provide the appropriate notice to insurers, and negotiate/litigate with the insurers regarding coverage in the event of a denial.

National Law Review, Volume V, Number 218