The recent revelation of the unauthorized disclosure of confidential National Security Agency (NSA) information to a British newspaper has brought to light the inherent risks of outsourcing top-secret intelligence work to private companies. Media reports have not only focused on the potential damage caused by the release of this data, but also the fact that the person responsible for providing that information was a civilian contract employee to the U.S. government.

Private industry has increasingly filled the personnel gaps created by the steady decline in the aging government workforce as well as addressed the rapidly changing technological competencies required to combat global terrorism. Companies that perform work for or on behalf of the federal government are likely examining the potential implications to their businesses if one of their own employees intentionally discloses top-secret or confidential information.

The current NSA scenario puts a new spin on the typical “rogue employee” fact pattern, where that employee accesses or discloses confidential third-party data in an unauthorized manner. Instead, this appears to be more of a whistleblower situation, where a contractor’s
employee breaches security through public allegations that the government is collecting private data in an illegal/unauthorized manner. In this instance, insureds should look to their brokers to discuss some of the foreseeable claims that might arise from this situation. We would envision several different policies that might come into play, including the errors and omissions (E&O), directors and officers (D&O) and employment practices liability policies.

E&O policies respond to claims across many potential insuring agreements including—but not limited to—technology services/products E&O, professional services, media liability, and network security/privacy liability. For claims that might be brought by the customer (in this case the client is presumably the NSA), companies may first look to the technology services/professional services E&O. Among other things, such claims might allege that the company failed to properly screen, supervise or monitor the employee in question, resulting in the release of classified information and whatever damages might be associated with that release.

From a privacy liability standpoint, the E&O policy can often include coverage for claims arising from the unauthorized disclosure of nonpublic personal information. This insuring agreement could be triggered if, for example, a plaintiff alleged that the insured was involved in the illegal collection and disclosure of private information. Typically such claims are brought in the form of a class action. The policy may also include coverage for privacy regulatory proceedings (e.g., a proceeding filed by a governmental authority in their official capacity, alleging violation of various privacy laws), as well as fines and penalties that might be levied in conjunction with such a proceeding. The policy may also include a sublimit for privacy event expenses, which are first-party expenses that the insured might incur in responding to a privacy event (such costs might include costs incurred to avoid reputational harm).

The primary D&O concern would be claims by shareholders alleging a loss in the value of their equity as a result of the public disclosure of such an event. While many D&O policies for technology companies may include professional services (E&O) exclusions, such exclusions should be tailored to allow coverage for securities claims arising from this type of situation. Such claims might allege failure by management to properly oversee and manage the engagement in question.

Another area to be considered is employment practices liability. We often see employment-related claims filed by whistleblowers following some form of punitive action or termination. In fact, a recurring fact pattern is that the employee is terminated first, and then files a whistleblower claim that really is nothing more than a trumped-up wrongful termination claim.
Finally, an emerging area of great interest to companies is the potential damage to brand and reputation. Contractors such as the one involved with the NSA leak depend, in large part, on contracts with the U.S. federal government. Unless an audit turns up an egregious error on the company’s part with respect to their employee screening and vetting policies, existing contracts are likely safe from being terminated. However, the potential impact to the organization’s ability to procure future business that involves classified or top-secret data is material.

Until recently, the commercial insurance market has been reticent to provide coverage for loss of or damage to brand and reputation. However, the London market has expressed a growing interest in pursuing this evolving area of risk. Led by Lockton, innovative carriers are providing policies to cover the loss of net profit (and extra expense) that is suffered following negative publicity. The triggers are flexible, tailored to each insured and agreed in advance to provide contract certainty.

Keep in mind that all insurance policies are subject to specific terms, conditions, exclusions and other limitations that may come into play depending on how specific claims are styled and how the various carriers interpret their policies when presented with such claims.

The recent events at the NSA have provided an opportunity for companies to reexamine how their risk management program would respond in the event one of their employees releases confidential information. Until now, the potential claim scenarios often involved the unintentional mistake or random human error. Current events have provided organizations with another area of concern.
Our Mission

To be the worldwide value and service leader in insurance brokerage, employee benefits, and risk management

Our Goal

To be the best place to do business and to work