LEGAL ADVISOR

A PilieroMazza Update for Federal Contractors and Commercial Businesses

Data Breaches and Data Rights: How the Rights of You and Your Customers Are Impacted

By Cy Alba

Data is ubiquitous. This means that the risk of theft, or simple loss, continues to increase as more information is stored in less secure and decentralized systems. While what we see in the news is usually focused on intrusions that reveal consumer/user information (such as personally identifiable information (PII), personal health information (PHA) under HIPAA, passwords, or similar data) the risk of intellectual property (IP) loss could be even more problematic and costly. This is especially true if you are using third party IP to perform work. In such cases, a breach likely means not only an embarrassing situation, but also a breach of license agreements and/or non-disclosure agreements that could cause you to lose the ability to access the IP entirely and expose you to liability for the loss. If that IP is critical to contract performance, you then risk termination for cause, financial penalties, and poor past performance assessments. These consequential losses can last for years.

If, by example, a prime contractor is using third party code via a traditional license agreement, and uses that code to build software for government use, there are a few issues that could arise. The first concerns ownership and licensing. For that reason, the prime and subcontractor need to understand the ownership and license requirements in the FAR/DFARS. For example, if the prime contractor is using commercial software developed at 100% subcontractor expense prior to performance, and the prime contractor has a license agreement with the subcontractor, the prime contractor should ensure that the license agreement terms are passed to the government. If the terms were not passed on to the government, the prime contractor may be in breach. Notably, it is possible for a prime contractor to constructively promise the government unlimited rights in data or software without having the rights from the subcontractor. In the example above, if the prime contractor did not pass on the license terms, the government's default position is that it takes unlimited rights in all software delivered, or even developed but not delivered, in performance of the contract. In the case where a prime contractor does not have such rights, the prime contractor breaches its contract with the government, but also its license agreement (most likely) with the subcontractor that provided the code. The prime contractor is then in a position of possible double liability, especially if the government shares the information with another contractor, acting under the assumption that it has unlimited rights. While this situation is similar to a data breach caused by hacking, what distinguishes it is that it was completely within the prime contractor's control and should have been prevented.

Second, and more directly to the point, a prime contractor can run into the same type of liability if it fails to follow the cybersecurity requirements in the contract. As noted, you will certainly be in breach of contract if you are hacked and you failed to follow the express requirements. There are additional cybersecurity requirements contractors should be aware of. For example, the contract may reference agency policies. In those cases, depending on the language of the contract, a failure to follow that guidance may also be a breach. Adding third parties only adds complexity. If you have no idea who actually hacked your systems or where that data resides, then it can be nearly impossible to stop its spread or even identify the scope of the leak and its impacts. If you signed a license agreement with a software company, as in the example discussed

Continued on page 2

PILIERO MAZZA

above, the software company may assume that the IP has been delivered to competitors, or hostile countries who may try and either use the code to develop its own competitor, sell the information to others, or use it to compromise government systems. All of that will cause large losses for the subcontractor, and it will certainly hold the prime responsible for the breach.

Additionally, the software license agreements may also have provisions providing for liquidated damages or presumed damages. In these cases, the prime contractor may have to expend significant funds to mitigate the leak, but also be on the hook for specific dollar amounts for each day the leaked information is not retrieved and such retrieval verified. Such verification may be impossible, in which case the subcontractor may attempt to recover much more than the value of the data/software itself. Courts certainly act in such cases and often refuse to allow such massive recoveries, but only after briefing on the case and, in some cases, costly discovery. Thus, as with all things, a penny of prevention is worth a pound of cure (or many pounds in this case).

Lastly, if the data was classified, there are a host of other concerns. First and foremost, there could be criminal violations, but, even putting that aside, the DoD's rules for spillage of classified information can make the contractor liable for clean-up. If the prime contractor has no idea who took the information or where it is, the attempts at clean-up can cost an infinite amount of money and resources, and it will be impossible to effectively determine the scope of the breach or the efficacy of the clean-up performed. Once that information is out on the internet, it is nearly impossible to track down and eliminate. As such, the government will likely undertake extensive measures, and it may charge the contractor for such attempts. Just one such incident can bankrupt even the largest company, much less small to mid-sized firms working on tight budgets. It should also be mentioned that while insurance can help cover perhaps $1M in losses, perhaps a few million, depending on the policy, the consequential damages are sometimes exempted from coverage or, even if covered, would not come close to the amounts necessary. For these reasons, on classified contracts, it is imperative that you have a robust system that meets all contractual requirements and other standards.

In sum, a data breach is not just about leakage of sensitive information, but may also be much more serious and more difficult to address. If you are working with highly proprietary IP from vendors and subcontractors (or the government itself), such a leak can bankrupt a company, result in litigation, or provide the basis for poor past performance reviews. For these reasons, it is critical that companies understand their cybersecurity requirements and those imposed on them by license agreements and subcontracts so that they are not taken by surprise if an incident happens, and so they have solid defenses against claims by licensors or the government.

About the Author: Cy Alba is a partner and is a member of the Government Contracts and Small Business Programs Groups. He may be reached at ialba@pilieromazza.com.