The Ins and Outs of Cyber Liability Insurance

By Thomas H. Bentz Jr.

Losses from cyber events can be staggering for government contractors. Attacks, often from nation-state-sponsored entities, can cause millions of dollars in losses and be devastating for a business.

For example, in 2014, a high-profile provider of background checks to the Office of Personnel Management experienced theft that allegedly exposed the personal information of about 27,000 government employees.

OPM terminated its contract, resulting in $417 million in lost revenue, and the contractor's parent company was forced to file for bankruptcy protections. This was in addition to the cost to notify the employees of the breach, the costs of the related litigation and the damage to the reputation of the contractor.

Cyber liability insurance may offer a lifeline to government contractors to minimize financial losses in the event of a breach. Unfortunately, such policies are both complicated and rapidly changing. There is no standard policy form, which means that the coverage offered by one insurer can — and often does — differ dramatically from that offered by another insurer.

There is also little agreement between insurers on what should be covered, when the coverage should be triggered or even how basic terms should be defined. These differences make understanding what is and is not covered very difficult. It also makes it nearly impossible — or at least foolish — to purchase this coverage based on price alone.

One of the biggest challenges for government contractors trying to purchase cyber insurance coverage is simply knowing what to ask for from an insurer. There are many areas where government contractors should negotiate changes to their cyber liability insurance policies.

A typical prior acts exclusion excludes coverage for any claim based upon wrongful acts that occurred prior to a certain date — often the inception date of the policy. This can be extremely problematic in the cyber context because hackers may install spyware, viruses and other malware long before a breach is discovered. If the policy considers the intrusion date as the date of the wrongful act, a contractor may end up with no coverage for a breach that is discovered after the policy has incepted. For this reason, contractors should make every effort to avoid prior acts exclusions whenever possible.

Many government contractors are surprised to learn that cyber liability policies generally exclude coverage for portable electronic devices such as laptop computers or cell phones. Obviously, this can severely limit the coverage provided by a policy. Fortunately, many insurers will remove this exclusion if a contractor agrees to provide "satisfactory" encryption for any data contained on the portable devices — something most government contractors do already.

ISTOCK

Cyber liability policies often exclude coverage for any claim "arising out of, based upon or attributable to" property damage and bodily injury. This is too broad for many government contractors. Instead, the quoted language should be replaced with the word "for."

This change is important because, although a cyber policy is not intended to cover general liability exposures such as bodily injury or property damage, it must still be able to respond to claims based on the breach that do not involve bodily injury or property damage directly — even if such losses were also caused by the intrusion.

The bodily injury/property damage exclusion should also include a carve back for mental anguish, emotional distress and shock caused by a cyber event. Plaintiffs may allege these types of damages after a breach of their personal information. Many insurers will only provide this coverage upon request.

The mechanical/electrical failure exclusion removes coverage for claims caused by a mechanical shutdown such as when your computer stops working. This exclusion needs to be limited so that if a criminal causes the mechanical failure or shutdown by means of a virus, spam attack, etc., the policy may respond.

Many cyber policies exclude coverage for claims involving acts of war, invasion, insurrection, terrorism, etc. Including terrorism in this exclusion can be problematic in this context as almost all cyber attacks could be considered acts of terrorism whether foreign or domestic. This is especially true for government contractors that may be attacked by a nation-state entity. A strong cyber policy should not reference terrorism in this exclusion.

Cyber liability policies often exclude coverage for employment practices claims. If a cyber policy has this type of exclusion, contractors should make sure that there is a carve back for employment claims alleging privacy violations caused by a data breach.

Similar to the employment practices exclusion described above, a strong cyber liability policy will have a carve

back to the Employee Retirement Income Security Act exclusion for claims alleging damages caused by a data breach of the contractor's employee benefits program.

Most cyber policies include exclusions for fraud, intentional and illegal misconduct. How a policy determines whether a conduct exclusion applies, when that determination may be made, and who gets to make this determination is extremely important.

For this reason, many contractors prefer a "final, non-appealable adjudication in the underlying action" standard. This standard provides individuals with the maximum coverage possible and requires a final, non-appealable adjudication by a court in the underlying action to establish that the alleged wrongful conduct occurred. Without such a final non-appealable adjudication of wrongful conduct, the exclusion does not apply — for instance, when there is coverage available from the policy.

The insured vs. insured exclusion states that the policy will not cover a claim made by one insured against another insured. However, many cyber liability insurers will agree to "carve out" certain insured vs. insured claims for various reasons including for the following: failure to protect confidential information; failure to disclose a breach event in violation of law; the unintentional failure to comply with the insured's privacy policy; and violations of privacy statutes.

Often these carve backs only relate to a specific coverage grant so it is important to review each coverage grant separately.

Finally, in order to make sure that the acts of one insured person do not impact coverage for other innocent insured, a cyber liability insurance policy should contain an exclusion severability provision. An exclusion severability provision states that no wrongful act committed by any one insured shall be imputed to any other insured for purposes of determining the applicability of any of the exclusions.

There are a number of cyber liability insurance policies available today and they are highly negotiable. **ND**

Thomas H. Bentz is a partner at Holland & Knight LLP, Washington, D.C.

New Ecosystem Emerging In Military Logistics

By Graham Grose

The global defense market is emerging from the challenges it faced over the last five years.

In the Asia-Pacific region, sustained economic development and industrial and social maturity is leading to projected increases in defense expenditure. In Western markets, the budgetary cutbacks of recent years have passed their peak, and in some countries, such as the United Kingdom, there are projected increases in defense expenditures.

Major military conflicts are waning, while being counter-balanced by significant increases in terrorist-based, insurgency-type operations.

Without a doubt, the growth in machine-to-machine and connected devices, along with the transformational power of emerging technologies and revolutionary arrivals such as the F-35 joint strike fighter are going to change the military support environment.

We will start to see the growth of demanding ecosystems involving multiple relationships between contractors and manufacturers based on complex contractual agreements and varying levels of capabilities. These "protected" military ecosystems are likely to result in a more concentrated defense manufacturing market. The more protected ecosystems there are, the more competitive it will be for tier-two manufacturers to play roles as suppliers.

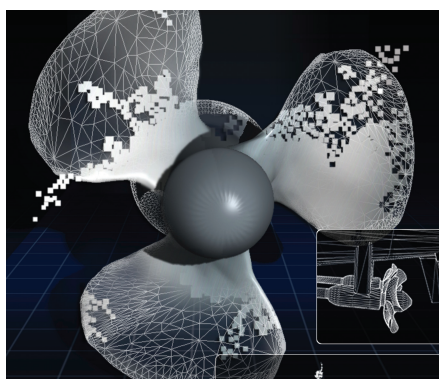
There are some key developments that will change the way defense organizations will operate and, in turn, bring huge changes to military support chains.

First, new technologies offer promising advantages for defense organizations, helping keep control and full visibility at every step in the support chain. Connected devices are now playing a big role in maintenance hangars. The next generation of warplane has arrived in the F-35, and military logistics needs to move with this. An F-35 has internal and external sensors that send real-time data to a ground-based logistics support system, which then seeks to optimize the end-to-end support chain. Hours can be saved in the maintenance bay by making sure the right equipment is available in the right place at the right time, so engineers are prepared for the task in hand and ready with the right part as soon as the aircraft lands.

The emergence of 3D printing, or additive manufacturing, has big potential for military ecosystems, perhaps more than most realize. The most obvious advantage is being able to produce parts when they are needed, meaning organizations can keep control of their support chains and end-to-end manufacturing processes by controlling distribution and quality of parts, affording increased opportunity for tier-two manufacturers.

Producing parts in theater, on what is now increasingly mobile 3D printing technology, means potentially spectacular advantages in the military context and a reduced logistics footprint in terms of not having to ship large, complex assets that are vulnerable to enemy attack over long distances. There is less risk associated with forecasting, less need to hold assets in large logistics parks and less staff involved in managing those assets and in managing the turnover.

For example, the U.S. Navy has adopted 3D printing technology on board the USS Essex to produce custom drones. Data files and models can be sent from land bases to ships hundreds of miles away and can be printed and fully oper-



"Technology such as 3D printing has the potential to cause disruption."

NAVY