HUNTON& WILLIAMS

Byline

June 29, 2015

The Risk of Insuring Supply Chains From Cyber Risk

by Lon A. Berk and Sergio F. Oehninger

Published in Law360

As the Internet of Things expands so too do supply chain-related cyber risks. Embedded software is incorporated into IoT products at different tiers of the supply chain and ordinary functionality testing may not disclose cybersecurity flaws. As one commentator observes:

> [M]any networks have been compromised by components with security flaws built into embedded software code. These flaws can be difficult to detect since they are usually masked by the proper functioning of the device.

The risk to manufacturers and distributors of IoT produces is nonetheless real.

> IoT device manage a huge quantity of information; they are capillary distributed in every industry and, unfortunately, their current level of security is still low.

Imagine the manufacturer of a "smart thermostat" connected to a home network. Perhaps it is designed to lower the temperature of a heating system when occupants are not detected in the home for a period of time. The chips supporting this functionality may have been supplied by one tier of the manufacturer's supply chain and may incorporate firmware designed by other parties as well. Questions about control of and access to this code thus become critical parts of the manufacturer's risk. Is the code available for analysis by hackers searching for flaws? Who has evaluated the firmware for flaws? Can a hacker access information through the thermostat to determine when a burglary of the home might succeed? Can a hacker control or access other devices on the network through a software flaw in the thermostat?

These questions are not merely theoretical. There have been reports of malware targeting IoT devices, including TV set-top boxes and of a botnet made up of IoT devices (called a "thingbot") being used by cybercriminals. It is not hard to imagine circumstances where victims of these cybercriminals blame manufacturers for security flaws in IoT products and seek compensation for resulting losses.

Manufacturers might try to transfer this exposure to different tiers of their supply chain through a series of indemnification and insurance agreements. For example, contracts with suppliers might require that the supplier indemnify the manufacturer for software as well as other flaws in components supplied. A natural corollary of this approach is to use cyberinsurance to bolster the manufacturer's protection, requiring suppliers to procure cyberinsurance and name the manufacturer as an additional insured.

A similar approach is used in the construction and other industries. Construction contracts commonly require subcontractors to procure insurance naming the general contractor as an additional insured, with similar requirements for sub-subcontractors. Through such mechanisms, the costs of errors in a

subcontractors' work are borne by the subcontractor and its insurers even if claims therefor are made against the general contractor. Such risk transfer mechanisms work in part because insurers have developed products sufficiently standardized to enable contractors and subs to reach agreement on what insurance to procure. Unfortunately, cyberinsurance has not yet been sufficiently standardized to function similarly and careful specification is needed if it is to function as a risk transfer device in supply chains.

There are (at least) two reasons a manufacturer might desire its suppliers to procure cyberinsurance. First, the manufacturer might desire the insurance as a hedge against the suppliers insolvency so that, in the event the manufacturer must look to the supplier for indemnification relating to a cyberevent, sufficient assets will be available and collectable. Second, the manufacturer might seek the insurance to protect itself from claimants as well. The first purpose is served by requiring the supplier to procure insurance covering indemnification claims by the manufacturer. To realize this purpose, any contractual liability exclusion must contain an exception for indemnification agreements such as that running from the supplier to the manufacturer. The second purpose is served by requiring the supplier to procure insurance identifying the manufacturer as an additional insured. However, both purposes cannot be simultaneously realized unless the cyberinsurance is structured correctly. In particular, for a supplier's cyberinsurance to function both as a hedge against the supplier's insolvency and as direct protection of the manufacturer, the insurance forms need to be carefully reviewed and, perhaps, revised.

Many cyberinsurance forms include cross-liability — or insured v. insured — exclusions, barring coverage for claims brought by one insured against another. If such an exclusion is present in a cyberinsurance policy, the policy cannot be used to simultaneously protect against supplier insolvency while independently providing coverage to the manufacturer. For example, one widely used cyberinsurance form contains an exclusion barring coverage of any claim:

> ... brought by or on behalf of: ... any other insured except, this [exclusion] shall not apply to a claim brought by an employee ...

If manufacturers were named as additional insureds under policies containing such an exclusion, their claims against suppliers might not be covered. In one case, for example, the general contractor on a construction project was indemnified by a subcontractor. When the general sued the subcontractor for negligence, the sub's insurer denied coverage contending that the general was an additional insured. The court agreed with the insurer, finding that the cross-liability exclusion barred coverage. If such precedents were applied, manufacturers named as additional insureds might not be able to use the insurance as protection against supplier insolvency as the manufacturer's claim against the supplier might be barred by the cross-liability exclusion. Where the supplier's assets are minimal or otherwise unreachable, the manufacturer could find itself financially responsible for the supplier's missteps.

Not all cyberinsurance forms contain such cross-liability exclusions. Some specifically except circumstances where suppliers are required to name manufacturers as additional insureds under contractual agreements. For instance, another widely used cyberinsurance form contains an insured v. insured exclusion that bars coverage for claims brought by or on behalf of:

> ... any insured ... provided, however this exclusion shall not apply to ... an insured [which the named insured is "required by contract to add as an insured ..."]

Such an exclusion should not bar coverage for claims by manufacturers against suppliers or others in the supply chain if the manufacturer was contractually required to be added as an additional insured. If cyberinsurance is to be used by the manufacturer to transfer supply chain risk, the insurance specifications in the agreement with suppliers need to be clear as to the nature of any cross-liability exclusions in the policy.

Of course, if a manufacturer finds an insurer contending that coverage is barred by a cross-liability exclusion contained in a supplier's policy, all is not necessarily lost. The purpose of these exclusions is to bar coverage for collusive litigation. In the directors' and officers' context, where the extent of these exclusions is often litigated, some courts have found that suits brought by a trustee on behalf of a corporation against its directors are not barred by the cross-liability exclusion because the suit is not collusive. For instance, where the U.S. Federal Deposit Insurance Corp. takes over a savings and loan institution and pursues claims on behalf of that institution against officers and directors, it has been found that a cross-liability exclusion does not bar coverage due to the absence of collusion.

> It is clear beyond doubt, and without requiring [the insurer] to engage in any close scrutiny, that [the FDIC's] involvement in the underlying actions is not collusive. The "insured v. insured" exclusion therefore does not excuse [the insurer] from coverage ...

Where a claim is brought by a manufacturer against a supplier arising out of a breach caused by a cybersecurity failure, the claim would not seem to be collusive and, arguably, should not be subject to a cross-liability exclusion. Nonetheless, this principle is by no means settled and manufacturers would be well advised to use it only as a last resort when seeking to shift financial responsibility for cyber risk arising out of their supply chain.

To sum up, as the IoT expands, so too do cyber risks created by the supply chain. Manufacturers looking to control that risk may seek indemnification and insurance protection from their suppliers. However, that strategy contains hidden risks. There are no settled cyberinsurance forms. Some may contain provisions undermining their use as supply chain protection. In this case, as in others, care must be taken to secure the correct form of insurance.

The Risk of Insuring Supply Chains From Cyber Risk
by Lon A. Berk and Sergio F. Oehninger
Law360 | June 29, 2015