BUSINESS INSURANCE.

Careful negotiations reduce risk of being held to cyber ransom

Posted On: May. 22, 2016 12:01 AM CST

James Westerlind and William Tanenbaum

Cyber attacks have become a major problem for businesses as they grow more sophisticated, frequent and lucrative. But a specific strain of malware has become a part of doing business for certain information technology vendors. James Westerlind and William Tanenbaum of Arent Fox L.L.P. discuss this use of software to lock up a client's account and how to successfully navigate it through use of contracts.

James Westerlind, left, and William Tanenbaum

Sixty percent of the victims of cyber attacks in 2014 were small to midsize businesses, according to Symantec Corp.'s, "2015 Internet Security Threat Report" issued in April. These were mainly ransomware attacks, where cyber criminals use malware to hijack a company's computer system and "sell" the data back to the company. Malware is destructive software that can be used not only by criminals looking to make a quick buck, but also by vendors who use a version of it lock up their software to provide leverage in a dispute.

Carefully crafted and executed contracts can limit the need for such drastic action.

Requests for proposals

It starts with requests for proposals issued by customers to vendors for information technology projects. They should be used strategically and as part of an end-to-end contract process. The customer has strong leverage during the RFP stage when vendors are competing for the engagement. Moreover, the RFPs should be designed so the responses correspond to important provisions in the contract and in the project plans and statements of work that cover specific technical services. As such, it is advantageous to treat RFPs as legal, as well as technical, documents.

Lawyers should be involved in drafting the RFP to require the vendors to respond promptly to customer needs on liability limits and implementation of cyber security measures. Lawyers also should review vendor RFP responses to advise the company of potential risks arising from legal protection limits the vendor seeks.

Most disputes arise under statements of work rather than overarching master service agreements. The SOWs are project plans that should set forth clear obligations, avoid shared responsibility between the customer and

the vendor, which will absolve the vendor of liability, and provide clear remedies.

An SOW is successful when a company asserts a failure and the vendor's legal department determines that it has responsibility under the agreement. The ultimate reader of SOW is a judge or an arbitrator, so the SOW should be drafted clearly with industry terminology defined and concisely to fit the analysis that a judge or arbitrator would apply to the dispute.

The vendor agreement and SOWs should permit the company to audit the vendor's security obligations and test the strength of vendor security features. Further, the agreement should require the vendor to correct any deficiencies promptly upon discovery.

Once these contracts are squared away, the company can move on to other areas of concern.

Third-party vendors

The company should have IT lawyers review existing contracts to see whether the technology requirements have become a ceiling, not a floor. A recent analysis by the Traverse City, Michigan-based consultant Ponemon Institute L.L.C. (which conducts independent research on data protection) found that two-thirds of data breaches come through third-party vendors. As the sophistication of malware attacks has increased, hackers have overcome the technology used only a few years ago. Accordingly, yesterday's contracts may not provide the protection against today's cyber threats. The contracts should then be renegotiated to update the protection the vendor must provide.

Cloud computing

Cloud services provide a special risk. Examples of cloud services commonly used by mid-size companies include Software-as-a-Service, where the company does not install or operate the software and an IT vendor sends the results to the company's computer systems. Cloud service providers often do not include security in their contract, opening an avenue of vulnerability. A solution is to obtain more security in the agreement with the cloud vendor.

Legal and audit protection

The company can also retain a cyber security firm to conduct a technical audit of its IT systems and vendor services to identify potential weaknesses. Besides closing doors to cyber criminals, there are attorney-client privilege advantages of having the cyber security firm work with a law firm, which can keep the results of an audit under wraps. This audit can find technical deficiencies in the company's computer operations and work with the attorneys and the company's IT staff and external vendors to fix them. The cyber security company can train the company's management and employees how to avoid being victims: Requiring employees to use more sophisticated passwords and avoid “phishing” attacks — deceptive emails with malware embedded in the attachments that infect the company's system when opened. Training to recognize suspicious intrusions must go all the way up a company's management, including its CEO.

Adequate cyber insurance

Besides taking all these steps, the company should purchase adequate cyber insurance, including data breach response coverage. These policies are relatively inexpensive and can provide the first- and third-party liability coverage that the company needs to weather a data breach or ransomware attack. The typical corporate general liability and property policies most companies purchase probably will not provide the coverage that the company will need in the event of a cyber attack. An appropriate cyber insurance policy will cover all or a portion of the costs and expenses that the company will incur in investigating a data breach, actual or suspected, notifying authorities and consumers of the matter and remedying the problem (including, among other things, providing coverage for public relations firms to assist the company in protecting its reputation following a data breach).

Many of the cyber risk insurers maintain a panel of professionals, including lawyers, forensic IT specialists, public relations firms and call centers to quickly assist the policyholder when a breach is suspected. The immediate assignment by the insurer to the policyholder of legal counsel who specializes in data breaches and notification laws has numerous benefits to the policyholder, including protecting communications with vendors assigned to assist with the matter as privileged and ensuring that each person involved in the breach response process is experienced and knowledgeable. One mistake early in the breach response could be devastating for the company, which, in most instances, is a victim itself.

Many insurers offer cyber insurance policies, and the coverage is not uniform. And many insurers offer additional coverages by endorsement, which must be requested and paid for (through additional, usually modest, premiums). An experienced insurance broker and coverage counsel can help a company select appropriate and adequate coverage.

In addition to obtaining its own policies, companies can require their IT vendors to purchase cyber insurance to spread the cost of mitigating risk and covering remedial action in a breach. The company should be named as an additional insured in the vendor's policies.

Legal review and technical audits help the company determine what insurance coverage it and its vendors should have, and these requirements should be specified in the governing agreements.

James Westerlind is of counsel on the insurance team at Arent Fox L.L.P. in New York. Contact him at 212-457-5462 or james.westerlind@arentfox.com (mailto:james.westerlind@arentfox.com) .

William Tanenbaum is a partner on the insurance team at Arent Fox L.L.P. in New York. Contact him at 212-484-3985 or william.tanenbaum@arentfox.com (mailto:william.tanenbaum@arentfox.com) .
