Cyber Insurance: Why You Should Require Certain Vendors to Have It

By: William C. Wagner, Taft Law

One way to protect your business from financial loss, reputational damage, and the expense of regulatory scrutiny in the event of a data breach is to require your vendors, with access to your customer and employee personally identifiable information, to carry cyber insurance.

Many businesses routinely require their vendors to promise to indemnify them from any loss or expense arising out of the vendor's goods or services. They also routinely require their vendors to maintain certain types and amounts of insurance coverage, have their business named as an additional insured under the vendor's insurance policies, and provide proof of the insurance coverage as conditions to their contracts.

But the types of losses, damages, and expenses that arise from a data breach are often not covered by the standard insurance policies listed in most vendor contracts. An instructive case to businesses on this issue is *Recall Total Information Management, Inc. v. Federal Insurance Co.*, which was recently affirmed by the Connecticut Supreme Court.

In that case, IBM entered into a contract with Recall to transport and store various IBM electronic media. IBM also required Recall to indemnify it from any loss or expense arising out of Recall's services. Later, Recall entered into a subcontract with Executive Logistics, Inc. for transportation services. Under the subcontract, Executive Logistics was required to maintain various insurance policies, including a $2 million commercial general liability policy and a $5 million umbrella liability policy, all naming Recall as an additional insured.

Unfortunately, during one of the transports, a cart containing 130 IBM computer tapes fell out of an Executive Logistics' van as it was exiting a highway ramp. The tapes contained personally identifiable information, such as names, social security numbers, birth dates, and contact information, for some 500,000 past and present IBM employees. Some unknown person retrieved the tapes, but the tapes were never properly recovered. Luckily, the tapes were encrypted and required specialized equipment for access to read the data on the tapes.

As you may know from our other blog posts, there is a patchwork of various state laws governing the types of notice that must be given to affected individuals, state attorneys general, and others in the event of a data breach. While some states do not require notification of a data breach to affected individuals where the information was encrypted, the encryption key remains safe, and the risk of disclosure is miniscule, other states require notification if there is simply any disclosure of personally identifiable information regardless of whether it is encrypted.

IBM took a cautious approach following the data breach of its employees' information. IBM spent $6.2 million in total to respond to the data breach. This included $2.5 million to notify the past and present employees of the breach, $600,000 to maintain a call center to answer their questions and concerns, and $3.1 million for credit monitoring services. IBM demanded that Recall indemnify it from these losses and expense, which Recall paid. Recall then made a demand to Executive Logistics and the insurers for reimbursement.

To make a long story short, the insurers denied Recall's claims on several grounds, including that there was no evidence that the personally identifiable information had been published, or was made known, to a third person. The Connecticut Court of Appeals and Supreme Court held that without evidence of a publication of private information, the policies' coverage had not been triggered.

In hindsight, Recall should have required its subcontractor (Executive Logistics) to maintain cyber insurance. Cyber insurance policies, among other things, typically cover the cost for computer and data loss restoration, notification costs, credit monitoring, and liability to third parties from your failure to handle, manage, store, and control personally identifiably information belonging to others. Recall and Executive Logistics could have also tried to limit their liability by capping their indemnity obligations to the amount of the contract, their existing insurance policy limits, or in other ways.

But the valuable lesson is that anytime a vendor has access to your customer or employee personally identifiable information, you need to have a discussion about sharing or transferring the risk of loss if there is a data breach, including through the use of cyber insurance.