CYBER CRIMES

Genuine risks for right of way service providers

BY PETER CHRISTENSEN

Virtually every contract these days for right of way services includes a list of detailed insurance requirements for the right of way service provider. Traditionally, the list has included coverages for professional and general liability, as well as workers compensation. More often, we are now also seeing insurance requirements for coverage of cyber security events – such as hacking or violations of privacy through accidental disclosure.

But are there actually genuine risks underlying these new cyber insurance requirements for companies engaged in typical right of way services? Two recent cyber-attacks on property data and appraisal firms would suggest that the answer is yes. The first attack—discussed below—was against the sophisticated, technologically-oriented company, CoreLogic. If an operation like CoreLogic can be victimized by criminal hackers seeking property information, as it was in an attack in February, any property service company is at risk. More seriously, the losses suffered by an appraisal firm in a separate cyber attack demonstrate how devastating the financial harm can be from an attack that spills valuation data onto the "dark web." That appraisal firm, with over 350 commercial and residential appraisers in Australia, has been suspended for new appraisal orders by the four biggest banks in that country and by other clients as well.

The Hacking of CoreLogic's Property Database

In February, the property analytics company, CoreLogic, filed a unique lawsuit in U.S. District Court, disclosing that it had been victimized by a malicious hacking of one of its property databases. The case is entitled *CoreLogic, Inc. v. John Does 1-10*. The reason that all of the defendants were identified in the lawsuit complaint as "John Does" was that CoreLogic did

not know the actual identity of any of the persons it was suing. All that CoreLogic knew about them was that they hacked into a CoreLogic database used for a property analytics application called "Risk Meter," copied the contents and stole the data by moving it to an external server. Additionally, it knew the IP addresses from which the attacks may have been staged.

Here is how CoreLogic described what happened in its complaint:

> *On or about February 7, 2019, one or more of John Does I-X used a SQL injection attack originating from the IP address 192.186.183.138 to obtain unauthorized access to and make copies of data used in application and client development that CoreLogic maintained on its Risk Meter development database.*
>
> *Shortly thereafter, on or about February 7, 2019, one or more of John Does 1-10 acted without authorization to exfiltrate the copied contents of the Risk Meter development database by downloading them to an FTP server located at IP address 104.168.99.29.*

CoreLogic says that the Risk Meter application provides "natural hazard risk reports and highly granular risk data, including data that could identify information associated with particular real properties." Within the stolen data were "client user identification and password information, user information, and real property data." It does not appear to be a critical or material problem for CoreLogic. There is no indication that any data spilled publicly or that it involved consumer records. That's probably because CoreLogic has a capable tech and legal team. Unfortunately, most smaller companies don't have the same resources to deal with criminal hackers.

The immediate action that CoreLogic's capable lawyers began pursuing was for permission from the federal court to serve subpoenas on the two web hosting companies associated with the IP addresses tied to the hackers. CoreLogic hoped that this would enable the hackers to be identified and that CoreLogic could then name them in the lawsuit to seek appropriate injunctions and damages.

Cyber Attack on Appraisal Software Platform

In a separate, more consequential matter, an appraisal firm LandMark White (LMW), one of the largest in Australia with over 350 appraisers, announced earlier this year that it had been victimized by an extensive cyber theft of data relating to valuation services performed over as much as an eight-year span from 2011 to 2019. In this incident, the company said that cyber thieves accessed the valuation data in one of the company's software platforms "via an exposed programming interface" and that the data ended up being made "publicly available on the dark web" by the thieves. Unfortunately, LandMark White also had to disclose that it failed to act on early warnings it received, including posts on Twitter about the hacked data.

LandMark White has indicated that the dataset contains, "approximately 137,500 unique valuation records, and approximately 1,680 supporting documents…approximately 250,000 individual records in total but a lot of records are duplicates… the date of the documents range between approximately 4 January 2011 and 20 January 2019. "

To say the least, this is a giant problem for the firm. For one thing, the firm has had to publish a notice to potentially affected consumers informing them: "If you are concerned, you should consider requesting that a 'credit ban' be put in place while you investigate further..." Australian news reports have indicated that the firm's clients may have to notify over 100 thousand borrowers. Another problem is that many of the firm's largest clients have suspended placing any further appraisal orders with the firm. The firm has stated, "We are unable to ascertain when these clients will reinstate LMW and hence when LMW will be in a position to assess with any certainty the financial impact of the incident." Finally, since the firm is a public company in Australia, after an immediate drop in its stock price as the attack became public, the trading in its stock was suspended. Its CEO has since resigned. If this had occurred in the United States, consumer and shareholder class actions surely would have followed next.

A Very Real Threat

That's the stark reality. Cyber threats are real risks to firms of all types, including those that handle property information and appraisal data. The risks concern both liability exposure and business economic losses. Any firm is certainly at risk, given that a powerhouse like CoreLogic itself can fall victim. At this point in time, however, cybercrime insurance coverage is neither difficult to obtain nor expensive for firms that provide services such as right of way service providers. Some experts have said that insurance carriers are not yet pricing the developing risk sufficiently. In other words, the coverage is a good value for the insured. ✪

Peter Christensen is General Counsel for LIA Administrators & Insurance Services and has been an attorney since 1993. Endorsed by the IRWA, LIA provides professional liability insurance and other types of insurance to right of way service providers.