# 9/11 documents hacked from insurers and lawyers

**Date published:** 02 January 2019

**Aliya Ram, Oliver Ralph and David Bond**

**Source: FT.com**

**Word count: 634**

**Link To FT.com:** [**https://www.ft.com/content/b39a8526-0eb2-11e9-a3aa-118c761d2745**](https://www.ft.com/content/b39a8526-0eb2-11e9-a3aa-118c761d2745)

The FBI is investigating the theft of 18,000 insurance and legal documents relating to the September 11 attacks on the World Trade Center by a hacker with a long record of holding companies to ransom, according to two people familiar with the matter.

Posting under the name “The Dark Overlord”, the hacker or hackers claimed on New Year’s Eve that they had taken emails and non-disclosure agreements relating to the 9/11 attacks that were sent and received by groups including insurers Hiscox and Lloyd’s of London and the law firm Blackwell Sanders Peper Martin, now called Husch Blackwell.

The Dark Overlord said it would sell the documents for bitcoin, inviting Isis, al-Qaeda and nation states to bid for them online.

On Wednesday, images of some of the documents began to circulate on the internet after the group released decryption keys. The images appeared to show communications relating to the World Trade Center.

The FBI and other law-enforcement agencies are now investigating the hack, according to people aware of the discussions that officials have had with the companies.

The Dark Overlord said it had been under investigation for years.

It added that it had also gathered other information from Lloyd’s and Silverstein Properties, a New York real estate developer that has owned and managed the World Trade Center since before the attacks in 2001.

Hiscox said it became aware last April that systems used by one of its legal advisers had been hacked.

“The law firm’s systems are not connected to Hiscox’s IT infrastructure and Hiscox’s own systems were unaffected by this incident,” a spokesperson said. “One of the cases the law firm handled for Hiscox and other insurers related to litigation arising from the events of 9/11, and we believe that information relating to this was stolen during that breach.”

The spokesperson added: “We will continue to work with law enforcement in both the UK and US on this matter.”

The September 11 attacks cost the insurance industry the equivalent of $45bn in 2017 terms, according to the Insurance Information Institute, and led to years of litigation over who should bear the cost.

Both Hiscox and Lloyd’s have expanded heavily into cyber insurance in recent years, selling protection against the costs of dealing with cyber attacks.

Husch Blackwell said it had not been hacked: “Several documents bearing the letterhead of a predecessor law firm to Husch Blackwell were made public earlier this week by a cyber terrorist group,” the company said in a statement.

“After a thorough review Husch Blackwell can confirm that no documents were obtained from Husch Blackwell and that there was no unauthorised access to Husch Blackwell systems, client files, documents or data.”

A Lloyd’s spokesperson said it had no evidence its systems had been compromised. “Lloyd’s will continue to monitor the situation closely, including working with managing agents targeted by the hacker group.”

A spokesperson for Silverstein said the company was investigating the claims. “We are aware of claims of alleged security breaches at firms involved in the five-year insurance litigation following the attacks of 9/11.

“To date, we have found no evidence to support a security breach at our company. We have spent the last 17 years fulfilling our obligation to deliver a magnificent and fully rebuilt World Trade Center. We will not be distracted by 9/11 conspiracy theories.”

The UK National Cyber Security Centre warned in 2017 that organisations with sensitive personal information such as medical institutions and law firms were at risk from The Dark Overlord. “Whilst evidence of the stolen data is often provided, the volume and sensitivity of the data may be exaggerated to maximise impact,” it said at the time. The NCSC added on Wednesday that it was aware of reports about the hack.

The FBI declined to comment.

*Additional reporting by Kadhim Shubber*

Copyright The Financial Times Limited 2019

© 2019 The Financial Times Ltd. All rights reserved. Please do not copy and paste FT articles and redistribute by email or post to the web.