Cyber crime going underreported as businesses cough up ransoms - often in bitcoin - for hackers to keep their data safe

3 March 2016 12:01am

by Hayley Kirton

"Cyber extortion is very common and it's been going on for quite a long time" (Source: Getty)

Businesses are paying out hefty cash ransoms to cyber criminals as they scramble to prevent online bandits from releasing large caches of their customers' stolen personal data.

Experts believe that several big firms have shelled out to hackers, often in the form of bitcoin, in order to save face and stop the data leaks going public.

"Cyber extortion is very common and it's been going on for quite a long time," Matthew Richardson, a barrister specialising in cyber crime at Henderson Chambers, told *City A.M.*, adding: "It's in the interest of companies who are extorted in such a fashion not to release the information that they've succumbed to that, because not only would it encourage further such extortion but also it damages consumer confidence."

A report released today by the Institute of Directors (IoD) and Barclays shows that just a quarter (28 per cent) of cyber attacks are reported to the authorities. Professor Richard Benham, author of the report, said that ransoms are often demanded in bitcoin as the transaction is harder to trace.

Benham told *City A.M.*: "You have very sensitive public companies with huge amounts of money and, with regard to their risk model, they would rather pay a ransom than suffer the reputational damage of people knowing that they'd been compromised."

Sarah Stephens, head of cyber at JLT Speciality, added: "I do think people would be surprised to know how often companies are paying ransoms. That behaviour is something that's shifted because it used to be that companies resisted paying."

Last year, the dating website Ashley Madison, which specialises in extramarital affairs, refused to give in to hackers' demands to shut down the site and customer data was subsequently leaked.

Benham believes that cybercrime "is one of the biggest business challenges of our generation and companies need to get real about the financial and reputational damage it can inflict".

Mark Weil, of insurance and risk management firm Marsh, told *City A.M.*: "There's no obligation to report and potentially no harm done if it's a foiled attack".

He added, however, that companies sharing information with the authorities could ultimately lead to the firms being better prepared against cybercrime.