Waterstons
we're with you

+44 345 094 0945
www.waterstons.com

Case study

Waterstons
we're with you

Service
Cyber Resilience

Oct 2022

Third party breach incident

We are more connected to our third-party suppliers than ever before; frequently sharing sensitive data to enable efficient business practices, as well as reaping the benefits of interconnected businesses.

Kieran Fowler
Head of Cyber Consulting
Email kieran.fowler@waterstons.com

As with all businesses, our clients trust other firms with their sensitive information, however some have learned the hard way that the security standards of these third parties didn't match their own.

The story below has been anonymised to protect the client.

"I received an e-mail from a trusted third party that simply said they were having an IT incident and that systems are temporarily down; 'thanks for letting me know' I thought and quickly moved on to my next e-mail.

"A few members of staff mentioned they were unable to use the service, so I let them know the situation. As it wasn't causing any real impact to us operationally, we simply expected to wait until they were back up and running.

"Later that day a more ominous e-mail arrived: 'We are currently facing a ransomware attack. We are working with our security partners to remedy the issue. We do not believe that any data has been stolen.'

"Ransomware attacks are relatively common, and this isn't the first instance of knowing someone hit with one, but another email arrived to say that they believe all data, including backups, was lost and copies in the hands of the hackers.

“I scrambled to consider all the data they held on us and how that can potentially be used to target our organisation.

“Luckily, we weren’t too exposed; the main issue being invoices believed lost could have been used to help facilitate fraud, with scammers replicating them with their own bank account details.

“The Waterstsons’ cyber team listened to the issue and provided training on how to identify this, and we also configured our email filtering to flag emails with the keywords of the third party so we could check them over before they landed in anyone’s inbox.

“Could we have stopped this? There’s no way we could have stopped the attack on a third party, but we might have been able to stop our business being impacted.

“This gave us the opportunity to identify improvements that needed to be made in how we manage our third parties, including:

- Knowing what data we were sharing, plus understanding what needs to be protected and why
- Understanding just how many suppliers and third parties we had across the business and how they are managed
- Discovering each supplier plus the data they had access to, enabling us to decide how we then protected it
- Having a conversation about how we want our data to be protected, and expectations when it came to incidents, moving to sending questionnaires and building requirements into contracts

“These conversations are critical to ensure we maintain our reputation; if our data is affected in a breach caused by a third party, it will be our name in the headlines.

“But having an understanding of our own security is only part of what we needed to do, and we are now much more comfortable in our understanding of our partners’ security, knowing they look after our data as well as we do.”

If you would like to understand and manage your supply chain risks, reach out to Waterstons cyber division to find out more about the supplier management toolkit, an effective tool to quickly manage your third party risks.

Email cyber@waterstons.com or visit the page here.