Waterstons
we're with you

+44 345 094 0945
www.waterstons.com

Case study

Service
Cyber Resilience

Oct 2022

Preparing for an attack

"We have a lot of security measures that look after us, what will I get out of creating an incident response team?" A client just months away from a cyber incident

Kieran Fowler
Head of Cyber Consulting

Email kieran.fowler@waterstons.com

We are currently in a cyber arms race. As capabilities in our defences evolve, our adversaries build new methods of attack, and some security measures that were effective in keeping us safe until just recently can now be bypassed. It's moving at such a pace that we need to run to stand still.

By accepting that we need to move from a 'protect only' mentality to one of 'protect and prepare' we can reduce the impact of an incident. That's exactly what one Waterstons client did just in time...

"We invested a lot into our security and had good measures and processes; we're Cyber Essentials Plus certified and close to obtaining ISO27001, but unfortunately a satellite office had a security incident that permitted an adversary onto our network. Despite all our efforts, we had a serious incident on our hands.

"Fortunately, we had only recently designed an incident response policy, and trained all members of our cyber security incident response team. This helped us to understand immediate actions that should be considered or undertaken. It also detailed roles and responsibilities so everyone knew who would be doing what, and we didn't waste precious time during the incident itself - when you are under attack every second is critical.

"Prior to this incident, we considered what would happen during an attack. This shifted our focus from stopping an incident from occurring, to detecting and investigating it. This was critical for us in understanding what was happening on our network, and ensuring that the attack could be stopped, and provide confidence that it would not happen again (as repeat attacks are common). We had assurance in our logs and, through our forensic partner, confirmed quickly the point of entry. The business had minimal impact and, for the vast majority, users were totally unaware of what was going on.

"Dedicating time to preparing for an attack helped us to minimise data loss and meant we had no customer impact. Admitting our security isn't flawless was a difficult conversation to hold internally but a necessary step to making us more secure which came just in time for us."

Information Security Manager, Global AEC organisation

If you want your business to be better prepared for an attack, get in touch with our Cyber Resilience team.