



**“The simulated attacks mean cyber security is always front of mind. Despite all the new attack techniques, we’re more secure now than we’ve ever been before.”**

Adam Davies\*, CISO, Financial Services

The financial sector has long been a target for cyber criminals. Which is precisely why **Adam Davies**, Chief Information Security Officer of a renowned UK high street bank, is constantly looking for new ways to keep customer data secure.

It’s also why, in 2016, Davies was searching for a new way to increase cyber security awareness within his organisation.

### Combating human error

“What was the case then, is still the case now,” he notes. “There are no two ways about it. The vast majority of cyber attacks are helped in some way by human error.”

As 2016 drew to a close, and as the number of breaches making front page news slowly increased, Davies became increasingly concerned.

As CISO, he had to ensure every person within his organisation not only knew about potential threats, but recognised them in action. As he puts it:

**“Everyone received regular, up to date training, no matter who they were. But over time it became clear that training was no good unless it was retained and made a difference. It needed to actually go on and prevent breaches from happening in the first place.”**

Before the year was out, Davies discovered CybSafe.

### Simulated attacks

“I was already looking for something that offered simulated attacks,” Davies notes. “One of my team recommended it [CybSafe] initially. I did some of my own research and it wasn’t long before I gave them a call.” CybSafe’s simulated attacks – that bring cyber security out of the classroom and into the workplace – weren’t the only draw for the Chief Information Security Officer.

As Davies puts it, the platform’s unique focus on using behavioural sciences to change human behaviour was “exactly what the [bank’s Information Security] team had been trying to achieve.” Within the space of a few weeks, Davies introduced his organisation to CybSafe.

### A cloud-based platform, available on demand

**“Internal logistics aside, the rollout couldn’t really have been any more simple,” he now reports. “It’s all in the cloud, so it really is as simple as getting the right people to the right online site, no matter where they’re located. There’s even a mobile app for those on the move”.**

As you might expect, the training doesn’t stop once the modules have been completed. The bank’s employees are tested on a recurring basis; through a series of dummy attacks, through performance feedback and through further formal training.

### Making cyber security front of mind

“It’s exactly what I was after,” says Davies. “The simulated attacks mean cyber security is always front of mind. Despite all the new attack techniques, we’re more secure now than we’ve ever been before.”

Ultimately, CybSafe has changed the culture and working practices of Adam Davies’ bank. At a time when human error accounts for 62% of the data incidents reported to the ICO, it’s a feat worth celebrating.

\* Fictitious personal and organisational name used for case study purposes only