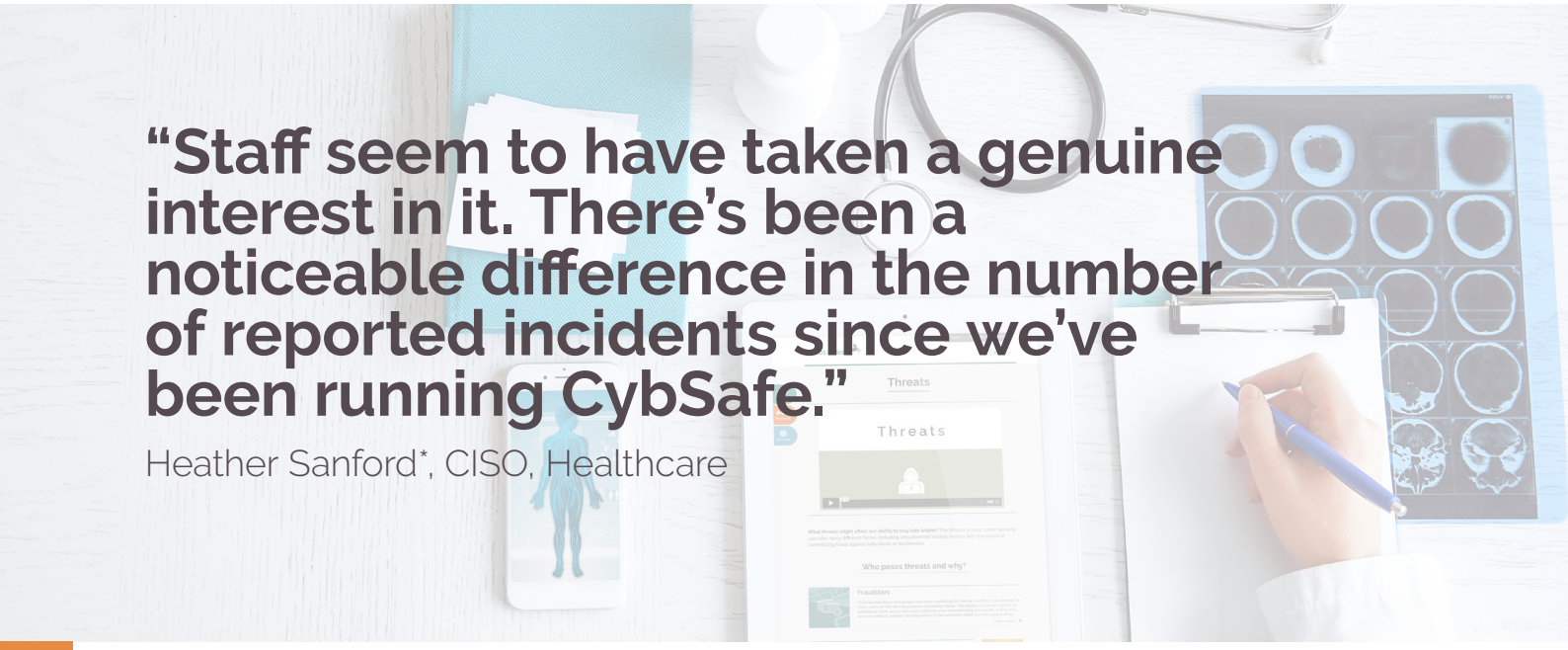

"Staff seem to have taken a genuine interest in it. There's been a noticeable difference in the number of reported incidents since we've been running CybSafe."

Heather Sanford*, CISO, Healthcare

In 2015, the healthcare sector experienced more cyber security incidents than any other industry. Over 100 million healthcare records were reportedly compromised in a period commentators have since labelled "the year of the healthcare breach".

As you'd expect, the news caught the attention of Heather Sanford, a Chief Information Security Officer employed by one of the world's largest private healthcare providers. "We have to keep hold of records for such a long time," says Sanford.

> "And, ultimately, a lot of our staff are focused on providing frontline healthcare. I'm pragmatic enough to know that **cyber security isn't always their primary concern**."

Making cyber security second nature

Sanford was aware that her company relied on talented people. But she was also aware of the cyber security risks preoccupied personnel posed – particularly given the rate of technological progress within her industry.

Given the variables, she decided educating her people to always follow best practice would maximise her firm's ROI. "I wanted cyber security to become second nature," she now says. "I wanted people to follow best practice without having to think."

She began to look for solutions that could make her vision a reality.

Building bespoke modules

Sanford knew she was looking for something different to the existing cyber security training program her company favoured. After several bouts of the same exercises, staff had begun to regard cyber security training as an annual inconvenience. "What I liked about CybSafe was it wasn't just the same thing with different words" Sanford says. "Instead of a list of what to do and what not to do, it focused on why. They even built us bespoke modules. It meant everything was applicable to healthcare."

Learning from analytics

Of equal use to Heather Sanford was CybSafe's analytics platform. Her company run a huge operation, and staff in certain areas seemed to take cyber security more seriously than others. As Sanford puts it:

> "The analytics and the simulated attacks show where we're most vulnerable, which means we can focus our efforts on the **areas that are weakest**. I also like the fact that I can compare myself to the rest of the industry."

The end result is noticeably fewer incidents across all areas of the organisation.

A noticeable difference

"Staff seem to have taken a genuine interest in it [CybSafe]," Sanford beams. "There's been a noticeable difference in the number of reported incidents since we've been running CybSafe. Way, way below where we once were and way below our key benchmarks... we're even looking at how CybSafe can reduce risks in our supply chain."

Combined with robust technological defences, CybSafe has decreased security incidents in both frequency and impact. As Heather Sanford once hoped, staff seemingly follow best practice without having to think.

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

CASE STUDY CASE STUDY