FORCEPOINT
POWERED BY Raytheon

Case Study

Chelsea and Westminster Hospital

"It is an investment to safeguard the patients; we are talking about you and me, our data being safe."

— Bill Gordon, Director of IMT, C&W

INDUSTRY
Healthcare

COUNTRY
United Kingdom

PRODUCT TYPE
Forcepoint Web Security, Forcepoint Email Security & Forcepoint DLP

SIZE
2,000 Users

SECURITY ISSUE
Data Leakage Incident

OVERVIEW

Opened in 1993, the Chelsea and Westminster Hospital (C&W) in southwest London is a 550-bed facility with a range of specialisms from pediatrics to dementia, serving 120,000 outpatients per year and a further 120,000 through the Accident and Emergency Department.

Over 60 staff members help Acting Director of IMT, Bill Gordon, to manage the IT infrastructure and all matters relating to patient records, clinical systems, networks, and desktop hardware. Data security has always been a priority, the hospital is currently the highest rated in the UK for IG (Information Governance), which covers the implementation of data safety and management procedures.

CHALLENGE

C&W was already a Forcepoint customer for web and email security as part of a comprehensive infrastructure that includes firewalls, encryption, and intrusion and hacking detection systems. An annual penetration test is run by NCC, a CESG-approved third party. Gordon says that C&W generally performs very well, encouraging confidence in the technology to steer behavior in the right direction.

Nevertheless, the impetus for change was a security breach – the loss of a USB key – which had to be reported to the ICO (Information Commissioner's Office). The incident had board-level visibility within the hospital that required an immediate response.

"We had a real incident and we needed to do something about it."

— Gordon

SOLUTION

Forcepoint DLP appeared to address the hospital's problem as it enabled the proactive management of data flows to help protect patients and their records.

"It was to give us visibility of who's doing what, when, why they are doing it, and where it is going."

— Gordon

The initial phase of building the DLP system involved C&W working closely with Forcepoint to assess and learn. From the millions of

pieces of data in play at any time, the process discovered which areas demanded careful monitoring and began to outline basic operating rules. Gordon comments that there were few surprises at this stage but the analysis revealed information on non-routine transactions.

"We could ask 'Why are you sending that file to that person?'"

— Gordon

The second phase defined the operating procedures more tightly. Every one of the 1.6 million patient records was "fingerprinted" so any movement could be monitored internally or, particularly, if it left the building. However, the security associated with blocking, encryption, and alerts had to be achieved without making the whole solution impracticable.

"If you make it unworkable, it will not be any use to anyone. We had to get a balance."

— Gordon

Forcepoint assisted C&W to configure templates given the nature of some medical subject matter that might otherwise be blocked automatically.

Finally, around a month was spent on implementation in collaboration with Foursys, a Forcepoint accredited business partner. Given the complexity of security installations, this was impressive, comments Gordon.

"It exceeded the expectation because it was quick."

— Gordon

RESULTS

Bill Gordon reports some outstanding initial results, alongside improved visibility and safety assurance. Previously, around 6,000-10,000 security incidents required investigation each month. Through rigorous filtering, this has reduced to just 10-20 that call for review by the hospital's IG manager, while other incidents, such as web browsing, are investigated by the C&W technical team. Most incidents are explicable, with a just a handful arising as a result of someone doing something they should not, observes Gordon.

"You need the buy-in from the business for any technical solution. Everywhere we can raise visibility, we do."

— Gordon

The implementation taught the hospital that engagement and internal marketing are crucial. Given the higher standards required by the ICO, the initial phases were accompanied by a variety of techniques including awareness campaigns, training, game-play, mystery shopping, and roadshows.

As a result, users quickly understood why, in order to protect patient data, certain actions were blocked or needed permission.

> "It does exactly what it says on the tin. It works."
>
> — Gordon

He now has evidence that the system runs smoothly, requires little maintenance, and provides the visibility required to monitor the flow of data in the hospital. He notes it is an evolving process with new versions planned that address social networking and the growing BYOD (Bring Your Own Device) issue as employees wish to connect with their personal iPads and smartphones.

Gordon notes that C&W has not performed an ROI analysis as the investment decision is so compelling.

> "If we lose data, we potentially have a fine of £500,000. We did not spend £500,000. It is an investment to safeguard the patients; we are talking about you and me, our data being safe."
>
> — Gordon

Chelsea and Westminster Hospital has relied on Forcepoint security solutions since 2007.

CONTACT
www.forcepoint.com/contact

ABOUT FORCEPOINT

[CASESTUDY_CHELSEA_WESTMINSTER_HOSPITAL_EN] 300010.021317