Softcat

Oxford Health NHS Foundation Trust

Case Study

Networking & security

# OXFORD HEALTH SAFEGUARDS SYSTEMS AND STAFF WITH MIMECAST

Community-focused organisation

Physical and mental health services

Eight community hospitals

Oxford Health NHS Foundation Trust, like most NHS Trusts, has seen a significant increase in recent years of cyber-attacks via staff email. Despite having successfully defended against the infamous WannaCry ransomware cyber-attack, the Trust was keen to ensure that it maintained the highest level of defence against cyber threats targeting staff.

## The Challenge

According to Colin Ingham, Server and Systems Consultant at the Trust not only had the volume of attacks been rising inexorably in recent years but the sophistication of phishing attacks using impersonation or email carrying malicious attachments or URL links had been rapidly increasing.

Unsurprisingly, the Trust has a high level strategic focus on cyber security and, as part of a planned migration from on-premise Microsoft Exchange to Office 365 in the cloud, it took the opportunity to further raise cyber protection on the organisation's virtual front door by rolling out Mimecast.

## The Solution

Having previously worked with Softcat for multiple security solutions, like web security and mobile device management, the Trust had built a long standing and strong relationship with Softcat. One of Softcat's Networking and Security Consultants undertook a robust research and evaluation process, in which they compared multiple solutions in this space. This both highlighted and recommended Software as a Service (SaaS) solutions to the Trust, based on the pros and cons of each service under review, helping the Trust to hone their focus on the right solution to prevent or limit email born cyber-attacks. Having reviewed Mimecast, Mark Walker, Head of IT for Oxford Health NHS Foundation Trust, decided that from the project outcomes Mimecast's email platform for e-mail Hygiene combined with its targeted threat protection (TTP) features was the right solution to safeguard them against cyber-attacks, targeting the Trusts 8,000 staff via their email as an entry point to the organisation.

As part of the TTP element within Mimecast, it identifies impersonation emails – which are designed to look like they are from a colleague, a superior or other trustworthy source. It also uses sandbox technology on e-mail borne attachments and Mimecast re-writes dubious URLs that could be sent via e-mail. This protects users who inadvertently clink on malicious links.

All 8,000 users now receive a digest three times a day, informing them of all spam caught by Mimecast and suspicious messages are held or marked as such. Users can review these emails via a personal portal and have the ability to release or block them. They can also flag senders as non-spam for future communications. The system won't however, allow them to unblock anything classed as malicious. In effect, the portal provides a safe space for staff to review suspect communications whilst unclogging their inboxes from potentially dangerous emails.

# The Benefits

Softcat's sophisticated approach has allowed The Trust to reduce their security problems. Through the implementation of Mimecast, real-time visibility has enabled Colin Ingham's team to flip the support paradigm towards proactive identification and resolution before users notice or report problems.

Since Softcat enrolled Mimecast to the Trust around 400% more spam and graymail emails were picked up during the first few months of implementation, compared to the months prior to roll out. As such, staff spend less time looking at spam, trying to work out whether it is safe to open or click. As Colin Ingham points out, even if that saves only five minutes a day for each user, when you add that up across 8,000 users the overall time saved for the Trust is significant. "It's time saved that gives our users more time to spend on supporting or delivering our organisation's primary mission – providing care for patients," said Colin Ingham, Server and Systems Consultant, Oxford Health NHS Foundation Trust.

Colin had assumed that the roll out would have issues but was pleasantly surprised that they received hardly any calls from their 8,000 users when they switched Mimecast on. He stated: "The initial implementation proved remarkably straightforward. We had access to high level support but Mimecast's implementation guides enabled us to be self-sufficient from very early on in the project. When we did need higher level support, Mimecast got back to me quickly, even out of office hours on occasions."

Benefits at a glance:

- Users now have more time to spend supporting and delivering the organisations primary mission.
- The implementation process was very simple and straightforward.

# Why Softcat?

Having worked with Softcat as a strategic partner for over 5 years now, when the Trust needed to look at a new e-mail security platform, they were the first choice for me. Softcat's independent view of the market combined with their knowledge of our infrastructure meant they would only put forward solutions fitting the Trust, saving us time in doing our own market research, which is an invaluable service to us as team. Softcat's breath of knowledge of IT and Cyber security coupled with their pragmatic approach to our requirements has always been the key reason we see them as our strategic partner in this area.

# Solution Highlights:

- Softcat's wide variety of Vendor's and dedication to helping The Trust allowed us to provide The Trust with Impartial and valuable advice on the right solution
- Users get a breakdown three times a day informing them of all spam caught by Mimecast and any suspicious messages are held or marked. This in turn has allowed users to be more empowered on their choice of e-mails they want to receive but also cuts down the time taken in deleting unwanted e-mails.
- The TTP element of the service allows IT at the Trust to rest assured that bogus impersonator e-mails can be captured, to stop staff being duped.
- The Sandbox and URL re-writing within TTP gives the IT support team vital visibility of the types of attacks that are being blocked and allow them to put better preventive controls in place.