Case Study

mimecast

NHS
Oxford Health
NHS Foundation Trust

# Protecting the Front Line from Cyber Attack

## Oxford Health NHS Foundation Trust has harnessed Mimecast to protect the organisation against cyber attack via the email front door

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

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.

### At a Glance

**Company:**

Oxford Health NHS Foundation Trust provides physical, mental health and social care for people of all ages across Oxfordshire, Buckinghamshire, Swindon, Wiltshire, Bath and North East Somerset. Services are delivered at community bases, hospitals, clinics and people's homes with focus on delivering care as close to home as possible.

**Products:**

- 2017 Mimecast S1 - Secure Email Gateway, Security & Compliance, 30-day Retention, Attachment Protect
- Large File Send and Secure Messaging add-ons
- 6000 users

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.

Colin says, "We had been manually intervening to protect the organisation from these attacks but the move to Office 365 provided the perfect opportunity to add a further layer of automated security to operations."

Following a robust research and evaluation process, the Trust is now using Mimecast's targeted threat protection features to safeguard against cyber attacks targeting its 8,000 staff via their email as an entry point to the organisation. It identifies impersonation emails – which are designed to look like they are from a colleague, a superior or other trustworthy source – captures and contains malicious attachments and neutralises suspect links within emails.

Users get a digest three times a day informing them of all spam caught by Mimecast and suspicious messages are held or marked as such. They can review these emails via a personal portal and have the ability to release or block them and 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.

## Flipping the support paradigm

Mimecast's automation, sophisticated reporting and real-time visibility has enabled Colin's team to flip the support paradigm towards proactive identification and resolution before users notice or report problems.

In addition, the ability to grant read only access to helpdesk and other support tiers to logs, monitoring and tracking has been incredibly useful, he adds. "This allows many issues to be dealt with immediately by first- and second-line support so that third line response teams can concentrate on genuine third line issues. This has helped us to spread and reduce the support overhead across teams.

"Now that we have tweaked Mimecast's protection, monitoring and notifications to our needs there's minimal admin overhead, which is beneficial as we do not have a team dedicated to mail security, it's a role shared amongst a team along with all other third line management tasks."

## Self-sufficient from roll-out

Colin had assumed that 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: "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 early on in the project. When we did need higher level support they got back to me quickly, even out of office hours on occasions.

"We were able to use most of the out of box settings and have subsequently customised protection, allowing for problematic messages and senders to be dealt with without needing to compromise global security settings."

Around 400% more spam and graymail was picked up by Mimecast during the first few months of implementation compared to the months prior to roll out – this meant that staff had to spend less time looking at spam, trying to work out whether it was safe to open or click. As Colin 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."

## Driving awareness, changing behavior

Mimecast's User Awareness feature has proved to be a useful bonus feature according to Colin: "Our users already have a high cyber security awareness as we've been working with them on this for some years - we regularly run random phishing tests for example - but we did see an improvement in users' ability to differentiate between harmful and safe links within a week of enabling the feature."

To keep security at the forefront of users' minds, Mimecast's awareness feature regularly nudges users to think about cyber security by asking them whether they think a particular email is 'safe' or 'a threat'. This nudge accompanies approximately five percent of messages and feedback from users is that they appreciate the gentle reminders to stop and think.

Indeed, feedback from users overall is positive. They like the flexibility Mimecast offers around blocking or permitting messages held by the system as spam and graymail. They also like the fact that most newly encountered spam and graymail is held by default, which means that they can be confident that external emails in their inbox are not just directly related to their work, but safe.

Overall Colin is very happy with the added protection provided by Mimecast. “During our initial selection review process, it was not only one of the market leaders, but it stood out with the simplicity and granularity of the console and information it provided.

It not only ticked all of our core requirements, as well as requirements for future opportunities, but it was competitively priced!”

“It has provided what it promised, and the roll out has been in our control, enabling us to implement safely, monitor and tweak at a rate that we were happy with.”

However, like the cyber-attackers themselves, Colin’s approach to security is one of evolution and he is continually looking to enhance protection. “Next year we plan to make use of Mimecast’s enhanced message encryption and Data Leak Protection features and build further on our use of built-in reporting to assist with DLP tasks and the ability to grant other teams access to such elements – this will allo w authorised information governance led teams direct access to messaging of interest to them, rather than involving technical services. We are also evaluating our requirements for mail archiving to enhance our message tracking and business continuity capabilities.”

In the meantime, however, Mimecast has allowed Colin to release staff time and let them focus on providing high quality healthcare in a safe and secure email environment.

*Mimecast is a cybersecurity and compliance provider that helps thousands of organizations worldwide make email safer, restore trust and strengthen cyber resilience. Mimecast’s expanded cloud suite enables organizations to implement a comprehensive cyber resilience strategy. From email and web security, archive and data protection, to awareness training, uptime assurance and more, Mimecast helps organizations stand strong in the face of cyberattacks, compliance risk, human error and technical failure.*