CASE STUDY

mimecast

Mayflower Group protects patient data by securing email

Mayflower Group is a social enterprise and not-for-profit organization dedicated to enhancing the independence, wellbeing, and lifestyle of older Australians. With more than 60 years of experience, Mayflower provides personalized in-home care services, state-of-the-art residential aged care homes, and retirement living options.

Founded in 1961 by volunteers from the Collins Street Independent Church, Mayflower's inaugural facility in Brighton began operations in 1963. Mayflower attributes its growth and success to the combined efforts of staff, volunteers, residents, donors, and board members.

Care without compromise

Michael Whyte is the ICT Manager at Mayflower Group. Michael says that Mayflower "provides care without compromise to enhance the quality-of-life choices for residents throughout their community." Michael has worked in healthcare for 15 years, citing his work as very rewarding and noting that he enjoys doing work that helps people with aging.

"We are all about people and our residents come first," Michael says of his work at Mayflower. "We could not operate without our amazing staff, but one of the most important aspects of our operation is protecting resident and staff data. Healthcare staff, while magnificent at providing care for patients, can also tend to not be the most tech savvy, so they need best-of-breed products to make sure they are operating at their best. Email protection is particularly important because this can be the weakest link."

Securing patient data is paramount

Healthcare organizations handle some of the most sensitive data imaginable: medical records, government-issued identification information, insurance details, and intimate health information that patients trust them to protect. This data is incredibly valuable to cybercriminals, who can sell medical records on the dark web for up to 10 times more than credit card information. As healthcare systems have digitized, moving from paper charts to electronic health records and implementing connected medical devices, they've created vast networks of interconnected systems that offer multiple entry points for malicious actors. This digital transformation, while improving patient care and operational efficiency, has also expanded the attack surface that healthcare organizations must defend.

One of the easiest points of entry to steal this information from healthcare facilities like Mayflower Group is through email compromise. Cybercriminals will target healthcare workers' inboxes with malicious emails containing links that download ransomware and other malware that allow them access to networks so they can harvest healthcare data on patients like Mayflower residents.

"Our staff are healthcare professionals – they are not office workers," Michael explains. "They are very busy on the floor and can be rushed and may not pay close enough attention when checking their emails. This can be problematic since it only takes one click of a malicious link to let in the bad guys."

> The beauty of Mimecast is that you can set and forget it. We have regular catch ups with our account manager, but the good thing is that the Mimecast team is proactive. This forces us to pay attention to the platform. The regular catch ups really keep us on track and using best practices. This is a distinct benefit for us. It gives us peace of mind."
>
> **- Michael Whyte , ICT Manager, Mayflower**

Securing email from compromise to protect patient data

Smaller healthcare organizations like Mayflower Group face unique cybersecurity challenges, with email serving as both a critical communication tool and a prime target for cybercriminals. Mimecast email security provides comprehensive protection that goes far beyond basic spam filtering, offering healthcare providers like Mayflower and healthcare data protectors like Michael the robust defense systems they need to safeguard sensitive patient information.

Mimecast's advanced threat detection capabilities identify and block sophisticated phishing attempts that specifically target healthcare organizations, preventing unauthorized access to electronic health records and personal patient data. With built-in encryption features and data loss prevention tools, Mimecast ensures that protected health information (PHI) remains secure during transmission, helping small healthcare practices maintain strict regulatory compliance without the complexity typically associated with enterprise-grade security solutions.

The operational benefits of Mimecast extend well beyond security, directly impacting the daily efficiency and trustworthiness that patients expect from their healthcare providers. By automatically filtering malicious emails and quarantining suspicious attachments, the system reduces IT workload and minimizes disruptions that could affect patient care schedules or critical communications between medical staff.

It's not just a product, it's a support community

"The beauty of Mimecast is that you can set and forget it," Michael says. "We have regular catch ups with our account manager, but the good thing is that the Mimecast team is proactive. This forces us to pay attention to the platform. The regular catch ups really keep us on track and using best practices. This is a distinct benefit for us. It gives us peace of mind."

"The regular catch up meetings also keep us informed of what Mimecast has coming down their pipeline," Michael added. "And the documentation Mimecast provides is also excellent."

Michael feels very positive about the support community that Mimecast has built for customers. "Having a partner like Mimecast that is focused on the human element is so important right now," Michael says. "With Mimecast, I get messaging that I can literally cut and paste into emails that I send to our employees."

Using Mimecast to handle human risk

Michael has a team of just four people to support over 600 healthcare workers at Mayflower. There is limited tech knowledge throughout the organization because people are focused on care, so Michael and his team must be the champions for security and using technology to deliver that security.

"I've been at Mayflower for two years," Michael explains. "Mimecast was already implemented when I arrived. This was my first time using it, and I was skeptical because I was a longtime Microsoft security user. I'm not normally

> One of the good things about Mimecast is how it handles human risk management. I am very happy about how comprehensive it is and the options we have to customize the solutions for our needs. Email security should not be about cost savings, but investing in the right platforms to ensure that the business process is secure. Security is much more important. I need to ensure we have good products, not inexpensive products."
>
> **–- Michael Whyte , ICT Manager, Mayflower**

one to sing a vendor's praises, but Mimecast has impressed me enough to do so."

"One of the good things about Mimecast," Michael continued, "is how it handles human risk management. I am very happy about how comprehensive it is and the options we have to customize the solutions for our needs. Email security should not be about cost savings, but investing in the right platforms to ensure that the business process is secure. Security is much more important. I need to ensure we have good products, not inexpensive products."

More ways Mimecast has benefited Mayflower

Michael is big on not creating a fear factor with the leadership at Mayflower. He creates a board report quarterly on potential issues that have been stopped. He doesn't want to create noise and keep people from doing their jobs, but believes being proactive is so much more important than being reactive. Michael also creates a regular email brief every two to three weeks to help keep security top of mind at Mayflower. When asked what he would say to a peer thinking about implementing Mimecast, Michael said, "I would tell them that Mimecast is best of breed when it comes to quarantining threats and securing email, and that the account check in process from Mimecast is so wonderful. It makes things easier to manage."

"We a quarantine a lot of emails," Michaels notes as well. "The staff is used to the process, which helps, and they have learned to take a look at those quarantined emails. They try to operate more safely. I'm not one to promote vendors, but Mimecast has really helped us with the process of securing our email. I wouldn't normally do a case study, but I was happy to do one for Mimecast."

Looking toward the future, Michael is hopeful that he can better integrate Mimecast into their existing security infrastructure and implement a single pane of glass for all their security solutions.

About Mimecast

Secure human risk with a unified platform.

Mimecast's connected human risk management platform prevents sophisticated threats that target human error. By gaining visibility into human risk across your collaboration landscape, you can protect your organization, safeguard critical data, and actively engage employees to reduce risk and enhance productivity.