Case Study

mimecast

Flexible cybersecurity awareness training for a diverse workforce

Including comedy and flexibility in a cyber awareness e-learning program wins executive buy in and excellent end-user engagement.

The Mater Group is a not-for-profit organisation operating across healthcare, education, fundraising and research. With a network of hospitals and health centres, Mater is the state's only nationally accredited hospital-based Registered Training Organisation and also operates a world-class research institute.

In 2017 a refocus of the ICT team saw Scott Hawkins appointed to the new role of Manager Cyber Security, Risk and Assurance. Coming from a business process background, Scott saw email security and cybersecurity awareness as top priorities.

At a Glance

- Supports 6500 email users
- Requirement for a flexible e-learning cyber security awareness training program that would appeal to a wide variety of users across the business

Company:

The Mater Group is a not-for-profit organisation operating across healthcare, education, fundraising and research. With a network of hospitals and health centres, Mater is the state's only nationally accredited hospital-based Registered Training Organisation and also operates a world-class research institute.

Products:

Mimecast Email Security and Mimecast Awareness Training

Benefits:

- Able to deliver regular cyber security awareness training at scale
- The engaging content in the program resulted in support at an exec level and as well as from various other stakeholders across the business which helped in successfully rolling-out of the program

"We had no e-learning available for training staff about cybersecurity" Scott says. "It was a real concern, as healthcare is often a target of cyber incidents and data breaches. Our most critical operations are keeping our core patient care systems up and running. Our focus was on the operational side of IT – keeping the lights on – but we hadn't done much to educate our 6,500 email users about cybersecurity threats to those same systems. In healthcare, patient care is mission-critical, so it's vital our core delivery systems are resilient."

Mater also needed a flexible training solution – given the wide variety of different users across the business. "A cookie-cutter approach wouldn't work. Our users have a wide range of roles and computer literacy levels."

Looking for an e-learning provider, Scott found large libraries of materials but little suited to an Australian audience. "There is lots of cybersecurity training content out there, but very little I'd feel comfortable putting before our people. Our staff undergo considerable training in their jobs and are required to absorb large amounts of information on a continuous basis, and we're competing with a lot of other key messages – so we must be able to engage them right from the start."

For this reason, Scott and the other stakeholders involved in the decision were drawn to the comedy angle in Mimecast's e-learning.

"IT had a big say about the way we'd go, but we set up a Cyber Awareness Working Party to evaluate our options. We're fortunate to have an education business within our group and leveraged their experience in assessing the best ways to approach cybersecurity training."

Scott says the reports from his Mimecast email security system are also very useful in educating end-users about the dangers of phishing. "When they realise how easy it is to get caught out, or if it happens to someone they work with, it's a great awareness opportunity. They're already well aware of the necessity of the critical systems we all rely on, and these reports help with highlighting the importance of patient privacy and data protection as well.

The selection process got stakeholders from across the business involved and engaged. According to Scott, "We've got excellent executive buy-in, because we've done a lot to educate the various stakeholders and I've seen strong interest since I have been in the role. I have had success sharing more relatable risks such as simple human error, as opposed to trying to scare them with horror stories from outside threats. It's easy to demonstrate how they could fall prey to such threats by accident themselves."

"We've come a long way in the past couple of years," Scott says. "Our approach is to start by talking about cybersecurity at home. When I walk into a room as someone from IT, their eyes are ready to glaze over, but getting them to check their personal email addresses on haveibeenpwned. com, seems to result in immediate engagement. Once they're interested, I link it back to Mater and the security of their work email and passwords. They're already well aware of the necessity of the critical systems we all rely on, as well as the importance of patient and employee privacy."

Scott and his team continue to educate people across the entire business. "At any given time, we have thousands of staff operating across many very different roles, which makes it an ongoing effort. The need for cyber awareness training won't ever stop."

"I have had success sharing more relatable risks such as simple human error, as opposed to trying to scare them with horror stories from outside threats."

Scott Hawkins,
Cyber Security, Risk and Assurance Manager, Mater