



Keeping confidentiality key, at Fisher & Paykel Finance

It's not just inbound email threats that keep Fisher & Paykel Finance Information Systems Manager Malcolm Jenkins awake at night. It's the potential for highly confidential customer and company information to leak out. Not many would want their financial details disclosed to anyone, let alone having in the wrong hands.

As a market leader in retail finance with its innovative Q Card and Farmers Card services, Fisher & Paykel Finance has solid business growth in equipment finance, and warranty and credit insurance. Which also means it holds confidential financial information for millions of customers - and as more and more of their business is done online, security of both inbound and outbound mail is critical.

So in 2013 when Malcolm was looking for a new email solution he was tightly focused on not only solving a raft of existing issues, but also putting in place a much more sophisticated environment: one which could finely balance individual user needs alongside the need to secure company and customer information from leaking, and at the same time exclude incoming threats.

"We were looking for a cost effective solution suitable for a finance company rather than an appliance company," he says.

"We wanted a reduction in our internet traffic and we wanted more flexibility and agility in tuning the system according to our business needs."

The existing in-house server-based system was failing in key areas, Malcolm says. It involved annual upgrade and licensing costs, support costs and high operational costs for email processing. It was part of shared infrastructure across the Fisher & Paykel businesses and was reliant on the Fisher & Paykel network being operational. If the network went down, mail was lost. Spam was filtered after it hit the Fisher & Paykel Finance network, with resulting bandwidth costs. But, most significantly, the existing system was inflexible.

"We were at a junction where people were fed up with the current rules that were put in place for good business reasons at the time, but now needed changing - which was too expensive and difficult. For example, we had a blanket

"Using SMX we've been able to put sophisticated rules in place so that users have different capabilities and limits appropriate to their role. This gives us the optimum balance of control, oversight and confidentiality."

Malcolm Jenkins

IS Manager

FISHER & PAYKEL FINANCE

ban on images, but with the advent of headers and footers on many emails there was a lot of email not getting through. We had to release mail with images entirely or get a smarter way to manage exceptions.

A big pain point was trying to manage content coming into the company in a smart way. There's a fine balance between IS responsibility to protect the organisation and IS providing an efficient mail service to employees. We were conflicted," Malcolm recalls.

Making the switch

Fisher & Paykel Finance went through a rigorous RFP and business case process, with key criteria being functionality, ease of deployment, and organisational fit and cost. Data sovereignty was also a consideration - "We need to know where our customer information is," Malcolm says. "It did bear on our decision that SMX holds our email in data centres in New Zealand. We were also impressed by the reporting features and by the capabilities of SMX's custom rules engine, giving us a powerful tool we could manage ourselves to safeguard our data and customise to different user groups.

SMX reseller Intellium managed the sale and implementation process, including optimising the SMX custom rules engine and reporting to meet Fisher & Paykel Finance's needs specifically.

"We found Intellium and SMX a very good team to deal with through and post the implementation, particularly with regard to just getting things done as necessary without frustrating paperwork and process delays. They worked the way we wanted to work. And that's the mark of a good IT services partner."

A step up to sophisticated email management

The shift to SMX solved or simplified a lot of their everyday email frustrations and management issues.

"For example, we have compliance requirements for auto responding to customer emails through the Financial Advisers Act. We were able to put fully compliant automated replies in place.

"We had more granularity. We had quick access to white lists and black lists, but found them largely superfluous as SMX already had it covered."

Malcolm was also impressed with the cost advantages that came with switching - a fixed per user, per month fee; no infrastructure costs, licensing costs or other one-off charges. Plus there was also a bandwidth benefit, with all spam filtered out before it hits their network.

"We were immediately freed from the frustration of a locked down email gateway filtering out any email with a header and footer - we fixed that on day one."

Using SMX's intuitive custom rules engine, Fisher & Paykel Finance's IS team streamlined the filtering on their inbound and outbound mail for all the different aspects of the business - call centre, sales, marketing, and back office.

"We've been able to put sophisticated rules in place so that different users have different capabilities and limits appropriate to their role. This gives us the optimum balance of control, oversight and confidentiality," Malcolm says.

"We also use the custom rules engine to identify the areas where we have data loss vulnerability and where inappropriate information is leaking out of the organisation. That information is used in a positive rather than a punitive way, as a guide for staff training and putting in place policies which strive to maintain an optimum balance between freedom to communicate and preservation of valuable information.

"We have confidential financial information on millions of customers. We are very serious and focused on protecting that information. It's all about continuous monitoring. There is no silver bullet. You have to work every day to continuously monitor and manage your risk.