CASE STUDY

mimecast

TIONG NAM

Tiong Nam secures users from constant email phishing and business email compromise attacks

The Asia-Pacific logistics and holding company was under constant attack from cybercriminals, attempting to gain a foothold through phishing and business email compromise attacks.

Company Name: Tiong Nam Logistics Holdings
Industry: Investment Holding
Company Size: 3000

For many years, Tiong Nam relied on open source email security, but when their first enterprise-grade solution was still allowing attacks to disrupt employee productivity, the company knew they needed to find a better solution.

Tiong Nam's Senior IT Manager and Information Security Officer sought a solution that would stop the disruptions while also bringing the company into compliance with government regulations and maintaining its competitive edge as a customer-centric service provider. The company was also seeking a vendor that focuses on human risk management.

The Company

Tiong Nam Logistics Holdings Berhad is an investment holding company based in Johor Bahru, Malaysia. As one of the largest total logistics service providers in the Asia-Pacific region, Tiong Nam has forged a reputation for efficiency, innovation, and service excellence.

Embracing integration has been key to the company's success, enabling it to grow from a transportation business, started in 1975, to one that today provides total logistics solutions, including warehousing, customs brokerage, cold room facilities, express delivery as well as crane and heavy transport services. Tiong Nam is also involved in renting of forklifts, trucks, and real estate property, including hotels, as well as providing courier services. In addition, other company operations consist of investment holding, the sale of goods, and the storage and management of empty shipping containers.

Since 2020, Tiong Nam's cybersecurity has been in the very capable hands of Keith Yong, Senior IT Manager and Information Security Officer, a 15-year veteran of the IT industry. Keith and his team of two are responsible for providing top-notch IT and cybersecurity for the entire organization, which consists of nearly 3,000 employees across 19 departments.

"We do a lot of things – impact a lot of areas," Keith commented when asked about what Tiong Nam does. "Each industry requires different logistics and solutions. Our needs are specific to the environment. In hospitality, for example, you get a lot of emails from booking sites, and many of these emails contain payment information.

The Problem

Like most modern transportation businesses, Tiong Nam handles a large volume of customer data and has a digital infrastructure that is critical to the successful operation and fulfilment of the company's services.

Tiong Nam is well known in Asia-Pacific, and its reputation as an important part of the shipping industry as well as its sheer size and diversity of business have all made the company a very attractive target for cybercriminals attempting to breach the company's security.

In addition, Tiong Nam needed an improved cybersecurity posture to meet government compliance and customer requirements from both the U.S. and E.U., and also so that it could remain competitive in a highly competitive market.

The company spent many years relying on an open source email infrastructure, but once it moved to a more enterprise-focused solution, they found it lacked true protection against modern threats like spoofing and business email compromise. This was a problem because Tiong Nam prides itself on delivering a customer-centric approach through which they maintain customer relationships by delighting customers and exceeding their expectations. Keith worried that a security breach could lead to financial loss or reputational damage for their customers as well as Tiong Nam.

Keith and his team evaluated several replacement solutions but found them lacking in usability relative to their cost. The functionality of the UI and the visibility into Tiong Nam's security environment was very important to Keith and his team, and they found most solutions lacking in this area as well. Keith chose Mimecast for its functionality and ability to visualize and respond to the **human risk** that exists within the organization, as well as Mimecast's ability to **integrate seamlessly** with their existing systems.

"Our users can be very unforgiving," Keith said. "If there is even one malicious or BEC email in an inbox, we can hear from users that our solution is not working. We needed a solution that was going to completely stop these spam emails from being delivered to inboxes."

The Solution

Mimecast was selected for its enterprise-grade security, **AI-driven threat detection**, and comprehensive email protection features. "Mimecast looked the best and had the best features," Keith commented.

> Plus, Keith was very impressed by Mimecast's ability to leverage AI to fight AI when it came to cybercriminals using the technology to craft phishing emails and **business email compromise** campaigns.

Mimecast's team provided professional onboarding support, thorough documentation, and hands-on assistance, including successful integration with Zimbra mail, a first in Southeast Asia. With the company's previous solution, users were seeing disruptions with their email that was negatively impacting their productivity. Mimecast changed all of that by stopping the disruptions and helping with the user comms needed to support implementation and user awareness of the new tools.

"The nice thing about Mimecast," Keith commented, "is that you don't have to be reminded of the product being used – it just works. Mimecast maximized the dollars and efforts that are put into implementing the solution, proved that it is the best, and delivered what we were looking for."

The Results

Tiong Nam achieved a robust cybersecurity posture, aligning with compliance and customer expectations. Mimecast's integration with Zimbra improved spam and threat detection, as well as impersonation protections, without disrupting user experience. Keith and his team were very satisfied with Mimecast's onboarding process, professionalism, and ongoing support.

Tiong Nam utilizes a number of Mimecast products and services, including **Email Security**, **Advanced Support**, **Analysis and Response Dashboard**, and the **Product Knowledge Hub and Education Program**.

"The Mimecast Command Center has been amazing," said Keith. "We are leveraging Mimecast to integrate across the board with our other solutions. A good product not only will achieve your goal but will work well with other products."

Overall, the implementation of Mimecast as Tiong Nam's human risk management provider was successful and well received. One year after implementation, Mimecast continues to conduct regular check-ins and updates to ensure optimal configuration.

"I have recommended Mimecast to a colleague I know would benefit from the same type of solution," Keith said. "The effort that was put into this project all paid off in the end. It proved Mimecast was the right solution. It proved that I made the right decision, which made me look good. The company put faith in me to find a solution and I feel that Mimecast delivers. My team feels proud of the work we have done, and the value Mimecast has added to the company. We didn't spend a lot, but we got some great benefits."

"Spam and phishing emails being stopped was key," Keith continued. "We stopped having to rescue users from making mistakes. The team got time back to focus on more important areas."

In addition to being happy with the performance of Mimecast's solution, Keith also feels the Mimecast team played a very important part in making the solution work. "The Mimecast team was always there, standing by, waiting to help and that made a big difference," Keith said. "The Mimecast team took the time to learned what we needed, and we felt very supported.

> "They helped us do the fine tuning, but there was not much tuning needed – the Mimecast solution just worked."

And once the Mimecast solution was implemented, Keith and his team worked with the Mimecast team to enable reporting right away. Keith and his team chose to review their reports monthly, delivering valuable insight. "We did not have any visibility like this before," Keith commented. "Complaints from users went down to zero. Mimecast's solution blocked what we needed it to block. It was super reliable."

Keith even discovered that in one of the months following implementation, his reporting indicated that the company had a surge of 600% in malicious emails. Keith says that they did not even notice the spike because Mimecast simply blocked all the additional malicious emails. "Imagine having a 600% spike in the volume of malicious email and still not even receiving a single user complaint," Keith said. "During the spike, one out of every two emails

we were receiving was spam and Mimecast just handled it."

Keith also noted that the automatic reporting they implemented allows him to more easily summarize the company's cybersecurity efforts and then send those results upwards to management, ultimately demonstrating cybersecurity.

The Future

When asked about what Keith will be focusing on in the future, he immediately commented that the organization is going to continue to focus on human risk when it comes to cybersecurity.

"I am very impressed that Mimecast is already focusing on human risk," Keith said. "Human risk is a big subject for us and is driving our strategy today. We are very mindful of human error and insider threats." Keith feels that for the foreseeable future, the company will need to put forth a lot of effort in this area. He says that the cost of products and how vendors support their products are important factors but moving forward he feels that products are going to be judged on how well they handle human risk.

> "Human factors are what we should be focusing on. Regardless of how much money you spend on top notch security products, all it takes is one click. This is the message I am spreading today. We must always work to protect the user. Mimecast is helping us do that."
>
> **–Keith Yong, Senior IT Manager and Information Security Officer**