Email: lifeline or deathtrap?

Picture this; you receive an email from your boss titled ‘important’, and it has an attachment. Naturally, you don’t think twice about opening it. But what you do not notice is that the email ID has a slight aberration, and it’s actually sent by a hacker trying to access your network. Most security breaches happen as quickly and simply as that.

Today email is the most important and widely used communication platform for organizations. And because of that, it’s also the most commonly used method of security breach.

For UST Global, the scenario is no different. As a Company that delivers digital, IT services and solutions to Global 1000 companies, security is of utmost importance.

With user mailboxes in the cloud and on premise, the mail flow configured for UST Global is pretty complex. The Company has to deal with large numbers of spam mails every single day, and controlling phishing attacks is a challenge in such a scenario.

Moreover the names and employee details of the Company’s top executives are available on various public sites, which makes it easier for attackers to use these names and email addresses to send out phishing emails.

UST Global was looking for a secure email gateway solution that could protect its complex mail flow configuration across the cloud and on premise. It wanted a solution that could handle the huge amount of inflow and outbound mails with its organization security check. Importantly, it wanted to control phishing emails.

Defending against advanced threats requires an advanced security solution

UST Global keeps attackers at bay with email security
The Cisco email security advantage

The Cisco email security solution was rolled out in 30 days, and it covers the Company’s entire email services. With the solution in place, UST Global found that:

- Spam flood has been controlled, email security checks are in-place as per the organization’s requirement.

- Phishing attacks through email are mitigated with DKIM (DomainKeys Identified Mail) and DMARC (Domain-based Message Authentication, Reporting and Conformance).

- The Company’s emails are better protected from viruses and malware, and filter settings have been configured for every user in the organization.

- In addition to all incoming and outgoing emails being scanned, there is also a TLS (Transport Layer Security) check for emails going out to customers.

- Employees feel safer, and the IT security team is satisfied with the security measures that have been applied at the email gateway solution. There is a tremendous increase in the mails that are captured by the threat analysis engines.

- The solution has given UST Global a wide variety of control options to configure the inflow and outflow of messages, monitoring inbound and outbound traffic for various threat analysis, malicious mails, legitimate mails, etc.

- Top executives are relieved that the malicious e-mails going out in their name have been minimized.

“Cisco Iron Port Security solution has been a class leading solution for the last decade. Cisco has shown its commitment to align with industry trends by providing the Iron Port SaaS platform for customers. This aligns very much with UST Global’s cloud & security strategy.”

Praveen Raveendran,
Head of IT, UST-Global.
In conclusion

Cisco Email Security has enabled UST Global to communicate securely. With this solution, the Company can now effectively combat business email compromise (BEC), ransomware, advanced malware, phishing, spam, and data loss with a multilayered approach to security.

“Cisco’s commitment to the security portfolio is evident from its security stack line staying on top of competition. Cisco chose UST as its first production customer to run the Iron Port stack in AWS cloud as part of the long standing relationship and trust.”

Sunil Kanchi,
Chief Information Officer and Senior Vice President, UST Global.