BIZCOMMUNITY

# Time for CIOs and CEOs to work together on email security

By Simeon Tassev

21 Jan 2016

Email is a vital communication medium for business but it also creates a doorway for potentially undesirable elements - from spam and malware to phishers and malicious threats.



While email security has traditionally been the territory of the IT department, the risk it represents to the business today makes it very much the CEO's problem too. It's time for CIOs and CEOs to work together on this challenge.

Everyone uses email. We assume it's safe because we use it from within a corporate firewall. Security is IT's responsibility, isn't it? The real answer is that there is no 100% secure email system. It takes awareness and ongoing vigilance by everyone using it.

## Exploiting security gaps

It's getting harder to put email security in place. With everyone making use of both private and corporate email accounts, and an endless mix of personal and business devices syncing these accounts across and between themselves, exploiting security gaps is becoming too easy. Vulnerabilities can result from numerous places - a lack of end-point protection on personal devices, an unencrypted email sent to a trusted entity, simple ignorance or malware or other threats that enters the business via employees' personal devices.

IT security best practices and policies can protect the business to some extent but the c-suite needs to take note of the new risks - and indeed the extent of the risk - that failed email security represents to the business. As we continue to digitise, it will take collaboration between the CEO, COO and CIO to identify risk and ensure the business is adequately protected. A balance must be struck between confidentiality, integrity and availability.

## Most important consideration

However, the most important consideration beyond best practices is that email security must be customised to how the company operates and how email is used within its processes. By auditing the organisation for potential risk, it can be

protected against those vulnerabilities.

• The first level of threat defence is usually via email hygiene or filtering solutions - a program that scans all email for threats, spam and viruses. This can be done in the cloud or, if the email server is on-premises, via a firewall gateway. A level of security may be installed on the email server, e.g. an anti-virus that scans email.
• Next, end point protection needs to be put in place on each and every device used by the employee, including personal devices that have some overlap with business functions. Users also need to be protected from human error such as sending a confidential email to a group rather than an individual.

• Continuity is also critical. Email headers and send/receive audit trails must be kept and be made secure against deletion or tampering.

• As complexity in the digital realm grows, targeted threat protection is gaining support. It's what will protect business email and data if users inadvertently click on an email harbouring a virus.

Security policies are essential. They form the foundation of any protection capability. However, to be effective they need to be regularly reviewed and updated and, above all, enforced. Staff need to be aware of potential vulnerabilities and new threats and be continually reminded. For best effect, security policies need to be supported top down - with the c-suite leading the way.

## ABOUT SIMEON TASSEV

Simeon Tassev is the director of Galix, a reseller of Mimecast Solutions in South Africa
- Cybersecurity awareness is no longer a generic exercise for business - 7 Feb 2023
- Understanding cybercrime's true impact is crucial to security in 2021 - 3 Feb 2021
- What can we do to stop ransomware attacks on governments? - 16 Dec 2019
- Cyber security professionals are no Darth Vader - 19 Mar 2019
- How to create a cybersecurity culture - 16 Jan 2019

View my profile and articles...