10 questions to help businesses assess their email systems

By Mary Shacklett
May 13, 2013, 11:58 AM PDT

Takeaway: Email is a critical communications tool, yet some organizations don’t give it the attention it needs. These questions will help you uncover oversights and develop better processes.

Email is an established business mainstay, but new challenges continue to emerge and old problems continue to exist. If you haven’t already done so, here are 10 questions to ask yourself about your office email.

1: Is email a mission-critical system?

Amazingly, most enterprise disaster recovery and business continuation plans don’t include email. But today, email is the bread-and-butter communication system in organizations. There is strong argument that email should make the mission-critical systems list.

2: How solid is our backup and recovery plan for email?

Many organizations are sloppy and even nonchalant with their email recovery and backup — especially if email is not on the mission-critical list. They shouldn’t be. Email today is the communications lifeline of organizations.

3: How long should email be retained?

This is a major question for organizations, especially since e-discovery used in legal proceedings demands access to email history. It is also important internally to maintain a history of emails, because it helps clarify communications. Finally, there are industry regulations that demand that organizations retain email (e.g., Sarbanes Oxley, HIPAA). Based on the requirements an organization is subject to, IT and end business users should define an appropriate email retention policy.

4: When do we take out the email trash?

Email is a major source of Big Data garbage accumulation. As an example, when a user sends an email with a large file attachment to a distribution list of 20 other recipients throughout the enterprise, that attachment gets copied multiple times on disk, eating up storage in the process. Techniques like deduplication exist to weed out unnecessary duplicate data. This is one way that IT can ensure more compact repositories of email history.

5: Do we need a dedicated server for email?

Many small and medium-size businesses (SMBs) combine email with other systems on the same server so they can maximize server capacity. But this amalgamation of systems on a single server can also complicate disaster recovery and failover for your email, rendering email unavailable for extended periods of time. Email is one system that presents a strong argument for a dedicated server because it is so vital to business communications.

6: Should we outsource email to the cloud?

Organizations are making the move to VDI (virtual desktop infrastructure) to save on software licensing fees, and some of this movement has also included email. However, as more companies begin to see their email as mission critical and not as a commodity office system, there is also movement to keep email as an internal system. IT managers need to weigh the cost and governance requirements of in-house email stewardship versus moving email to a third-party cloud hosting services.

7: What’s the best way to integrate email with other systems?

In recent years, organizations have moved to total integration of email with instant messaging, VoIP (voice over IP), and presence. The goal is anywhere-anytime instantaneous access to employees. Employees can also forward workflows from integrated messaging to others when they’re off grid. If you want this integration for your email but still don’t have it, the best way to get it is to find a vendor-business partner with the expertise to help you with your integration.

8: How clear is our email policy?

An email usage policy that gets reviewed annually with employees is a necessity, but most companies don’t do this. The consequences can be severe. A few years ago, I was managing IT and one of my company’s employees was getting bullied and threatened in emails from an old boyfriend who was an employee at another company. Ultimately, the ex-boyfriend lost his job. The company firing him had an email policy in place that it regularly reviewed with employees and that addressed his specific behavior, and what the consequences would be — so there was no misunderstanding.

9: Do employees understand that the company “owns” their email?

The First Amendment guarantees one’s right to privacy and also the right to free speech, but corporate email is a company asset. Employees need to be made aware that their communications via corporate email are for representing the company. Corporate email should not be used as private or personal email, and it should never be used to divulge corporate intellectual property without authorization. These practices should be stated in employee handbooks and regularly reinforced in annual training. Since IT, HR, and business managers are the ultimate enforcers when there is a breach of email policy, these areas should also be taking the lead to ensure that everyone in the company has a thorough, upfront understanding of corporate email position on privacy, intellectual property, etc.

10: Do we have a set of best practices for email automation?

Routinely, employees set email for automated messages: “I am out of the office and will return on Tuesday to answer my email.” If you have a corporate policy need to standardize which automation messages and practices employees are to use, these standards should be communicated to employees so employees are consistent in the ways that they use email automation