Meet the "New Standard" for Business Email

Email has been around for over 40 years and in that time, it has gone from being a "useful tool" to being a critically important business application.

Although the underlying technology has remained stable and proven during this time, the ecosystem around email has changed significantly and dramatically. New and unavoidable vulnerabilities have come to the forefront, making it crucial to take a fresh approach at managing email.

What's Wrong With The "Old" Way?

When the first email protocol was developed back in the 1970s, no one anticipated how important the technology would become to the world – particularly businesses. As a result, email wasn't inherently designed to address three major vulnerabilities seen today.

1) **The vulnerability of downtime.** It used to be that the occasional email outage was forgivable because mobile access was relatively rare and the business world hadn't yet developed the expectations of 24/7 access and immediate response time.

   Today, businesses need and expect their email to be always running—24/7 and 365 days per year. However, few businesses managing their own email servers can achieve that result. There are a number of reasons for this, including the inability:

   - To protect against local outages and disasters (cross-datacenter replication and redundancy are extremely complicated for on-premises servers)
   - To keep up with patches and updates that fix bugs and eliminate security holes
   - For individual administrators to offer 24/7 on-call service, which allows bugs to compound and increase in scale when nobody is on-call to fix them

   The bottom line: today's employees, customers, partners and suppliers have high expectations for the reliability of email. Anything less than 99.999% uptime – equal to less than a 30 seconds per month of downtime - puts everything at risk, including employee productivity, customer satisfaction, your business's reputation, and more.

2) **The vulnerability of email security.** Cybercriminals love the inherent vulnerability of email and they use a tactic called "spear phishing" to attack users. To perpetrate a spear phishing attack, a cybercriminal will send a user an email that appears to be legitimate, but is actually designed to

steal passwords, install malicious software, or worse. It has become so popular that nearly 95% of all attacks on the enterprise network are the result of successful spear phishing[1].

The protections provided by an Exchange server alone aren't strong enough to protect users against today's cyber-threats. As criminals get more and more sophisticated, email administrators must find new ways to combat these cyber-threats. Are the people managing your on-premises servers able to keep up with millions of cyber threats per quarter?

In addition to cyber security, physical security also needs to be considered because the facilities where servers are located may also be vulnerable. This is something many businesses don't think about until their offices are burglarized and their email servers are stolen. This happens more often than you think. And it's especially risky for regulated businesses, because this constitutes a data breach that may result in public disclosure and even fines.

3) **The vulnerability of data preservation.** Gartner estimates that about 45% of an organization's email provides some business value because the messages and attachments are related to a project, an initiative or are considered an official record.[2] What happens if an employee deletes an important message either accidentally or intentionally? How will you get it back?

Email was not designed to be "permanent." It is not inherently tamper-proof. You can't submit email as part of an "official record" in court unless it has been stored in a tamper-proof archive. How much do you stand to lose financially if you can't produce an archived message in court, or if the court is convinced that the message isn't admissible as evidence because it might have been altered? The risk is real: 82% of US businesses will be involved in some type of litigation[3] and you want all of your email to be available to bolster your case.

The "New Standard" for Business Email

To mitigate the risks inherent to today's email, your business must embrace these three key changes to your email infrastructure:

1. It should be hosted by experts in the cloud. For all the reasons listed above, more and more businesses are migrating their email from in-house email servers to the cloud. Your email needs to be managed by experts—including engineering specialists who can manage the complexities of cross data-center replication and backup; infrastructure experts who can ensure virtually no downtime; and trusted advisors that help assist with keeping day-to-day operations running smoothly.

2. It should be archived in a compliant, tamper-proof repository. Compliant email archiving isn't just for regulated businesses. When your email is properly archived, your data is stored in perpetuity with no ability to delete or modify the messages or attachments. Additionally, archived emails are indexed so

[1] Allen Paller, Director of Research, SANS Institute, 2013
[2] Best Practices for using email Archiving to Eliminate PST and Mailbox Quota Headaches, Sept 2012
[3] Norton Rose Fulbright 2015 Litigation Trends Annual Survey

they are easily retrievable and can be presented during eDiscovery, provided as part of an audit trail, or just restored to an active mailbox. With email archiving, your intellectual property is protected and, if necessary, stored in a form that a court of law will recognize.

3. It should be protected by advanced email security. The built-in protections of the standard email server are no longer enough. You have to protect your users and your business with a number of advanced security technologies, including real-time link scanning (in case a user clicks on a malicious link in a phishing email), inbound and outbound message filtering, and much more.

This "New Standard" offers a better way to approach the shortcomings of the old way—affordably. As you can see, it goes far beyond basic Exchange and delivers:

- **Higher reliability.** Moving your email to the cloud offers much greater reliability than a server in a closet. And cloud providers are experts at maintaining and securing email services. The best providers offer a 99.999% uptime service level agreement. This means that they're promising less than30 seconds of unplanned downtime a month.

- **Better security**. A hosted email provider is able to spend more resources on security measures than you would be able to provide on your own. This includes cyber security measures that deter phishing attacks and other online threats, as well as physical security to protect hardware from theft or damage.
- **Lower legal costs and better intellectual property protection**. In this day and age, it's imperative that every email and every attachment is preserved and protected. This will significantly reduce the cost of eDiscovery in the event of litigation. In addition, it will safeguard the intellectual property contained in your email against loss, even if an employee decides to clean out their all of their old emails.

Does your business meet the "New Standard"? Use the self-assessment test on the next page to see how vulnerable your company is.

Email Infrastructure	Do you have this capability? (Score 1 point for each Yes answer)
Best-in-breed hardware	
Always up-to-date server software	
24/7 on-call engineers	
Unlimited storage	
Accessible via any device	
Support	
Contract with Southridge Technology	
Business Continuity/Disaster Recovery	
99.999% uptime guarantee	
Backups to off-site datacenters	
Backup power	
Redundant ISPs	
Security	
Business-grade anti-virus/anti-malware	
Real-time URL scanning	
DDoS protection	
Physical security (CCTV cameras, keycard access control, etc.)	
Dedicated security staff & monitoring	
Intellectual property protection	
Tamper-proof archive of all emails and attachments	
Easily package emails to fulfill eDiscovery request	
Easily searchable archive of historic emails	
Your Score	____ out of 19

How did you do?

If you don't have a "1" in all the boxes your email your email could be at risk. To learn more or give us a call at 203-431-8324.

Southridge Technology
246 Federal Road
Brookfield CT 06804
support@southridgetech.com
203-431-8324