Why Email Fails

Dell Survey of Email Outages

Dell™ IT Management Software as a Service

THIS WHITE PAPER IS FOR INFORMATIONAL PURPOSES ONLY, AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND.

Executive summary

Email has become the most pervasive form of business communication, impacting every aspect of every organization: communications between management, employees, prospects, customers, vendors, suppliers, partners, investors, and analysts. According to Osterman Research, email traffic between 2008 and 2012 is projected to grow by 68%.[1]

Despite large enterprise investments in replication, mirroring, and tape backup systems, email systems continue to fail. While it is widely known that natural and man-made disasters can lead to email outages, new data shows that email systems are more frequently brought down by technological failures and human error.

Dell, a provider of email continuity, archiving and crisis communication services, conducted this research to understand the frequency and causes of email outages in North American corporations using Microsoft® Exchange Server. This research shows that enterprise email systems are prone to a variety of potential breakdowns including configuration errors, loss of network access, database corruption, SAN (Storage Area Network) failures, and viruses. Data from the survey shows that in any given 12-month time period, there is a 72% likelihood of an unplanned email outage and a 24% likelihood of a planned email outage for any given company.

This research report analyzes the leading causes of failure with enterprise email systems and provides preventative guidance to lower the probability of unplanned email outages.

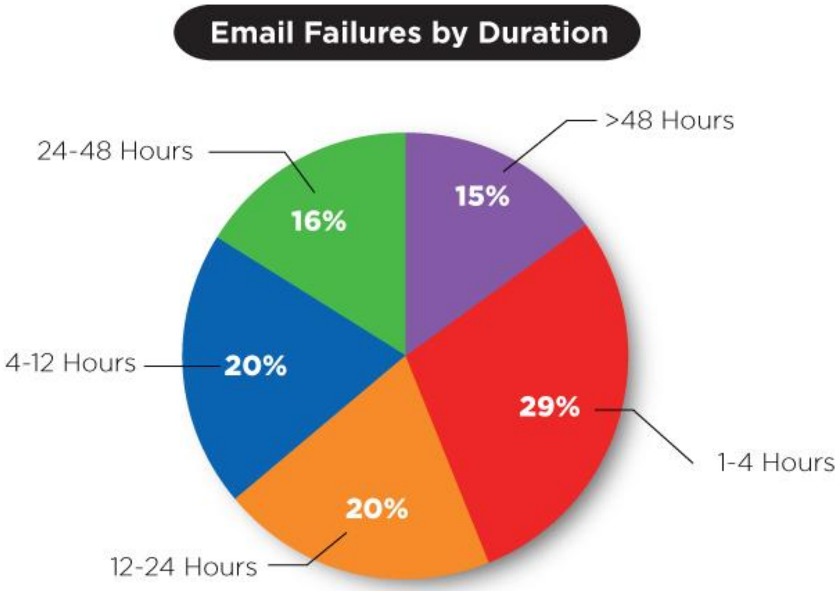
Dell survey results: email failures by cause

Dell provides hundreds of companies serving over a million email users with a highly scalable standby messaging system that can be activated in minutes at the customer's request, helping enable uninterrupted email services in the event that an organization's primary messaging system becomes unavailable or incapacitated.

Email Outage Frequency & Duration

Survey results show that in any given 12-month time period, there is a 72% likelihood of an unplanned email outage and a 24% likelihood of a planned email outage in any given company. Though the majority of these companies had stated Recovery Time Objectives (RTOs) of two hours or less, the length of email outages in the companies surveyed ranged from a minimum of 1 minute to a maximum of just under 2,000 hours with the average email outage being 62.2 hours long. The largest concentration of outages was between 4 and 24 hours in duration (40%). Approximately 16% of the outages lasted longer than 24 hours, a length of time that can lead to significant business disruption and damage.

Figure 1. US Disasters by Type

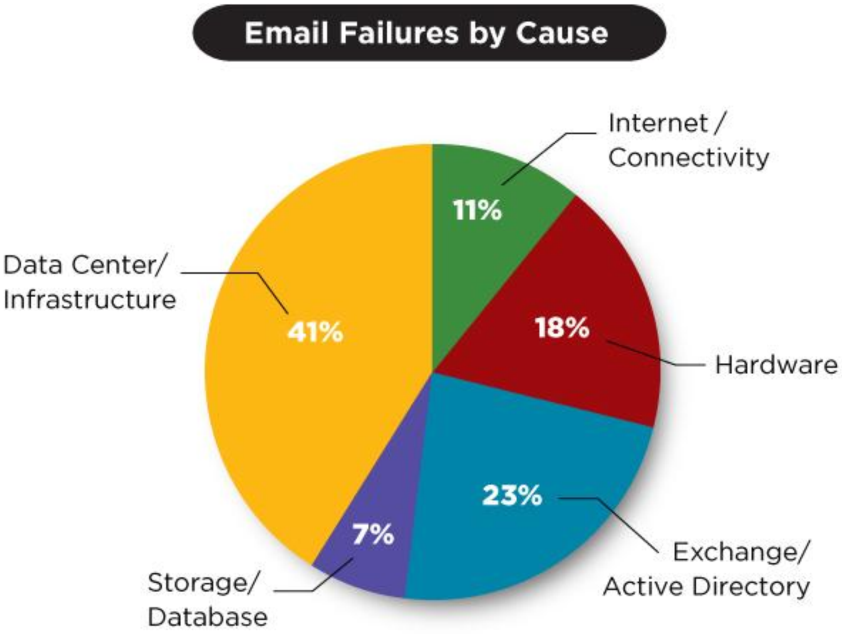


Email Outage Frequency & Duration

A majority of email outages are caused by unplanned events. Though natural disasters such as floods, tornadoes, and hurricanes often make the news, they typically account for only a fraction of the total events leading to email system failure. Technological errors are responsible for the majority of email system failures. Email software systems are complex ecosystems with many interwoven parts: server software, directories, authentication systems, etc.

The research results found that a large majority of email outages were caused by such unplanned technological failures. Of those failures, 41% of unplanned outages can be attributed to datacenter and infrastructure failures, such as power outages, HVAC issues, and water main breaks. These outages averaged 77.3 hours in duration. Exchange Server and Active Directory® issues accounted for 23% of the unplanned outages, averaging 15.5 hours in duration. Hardware failures accounted for 18% of all unplanned outages averaging 70.7 hours in duration. Internet and connectivity issues attributed to 11% of the unplanned outages, while storage and database issues accounted for 7% of unplanned outages.

Figure 2. Email Failure by Cause



Datacenter and Infrastructure Failure

Datacenter and infrastructure failure, a broad category, includes a variety of causations for email downtime. The most common type of infrastructure failure was power outages. Even with organizations that employ backup generators, the power blip was enough to cause the Exchange server to go down, thus interrupting email. Typically, however, the power outages, and other infrastructure failures such as water main breaks, caused extensive email downtime – on average over 75 hours which is an amount of time most organizations would find intolerable to be without email.

Exchange and Active Directory Failures

The risk of downtime associated with Microsoft Active Directory (AD) corruption was found readily apparent in our research accounting for roughly 23% of all email outages. Several customers experienced significant system-wide downtime as the result of Active Directory-related corruption. In each instance, Exchange-specific attributes or data was corrupted in a manner that disrupted communications. In several of these cases, identification, repair, and recovery resulted in outages exceeding 48 hours. Software-related email failure represented 14% of customer outages and was most commonly the result of configuration errors or software corruption. Other common causes included a mixture of technological failure and human error: faulty software patches, failed upgrade efforts, and failure from out of date drives.

Hardware Failure

A wide array of hardware and server related failures contributed to outages of customers. From catastrophic drive failure, to bad RAM (Random Access Memory), over a quarter of customer-related outages could be traced to hardware failure. In many of these scenarios, customers had already taken steps to mitigate hardware related issues by building highly redundant servers, including dual backplanes, and redundant RAID (Redundant Array of Independent Discs) controllers.

Several items of note:

- Branch office messaging servers were often not as fully redundant as their datacenter counterparts.
- New hardware or recently upgraded hardware was more commonly the source of server related outages.
- Server sizing issues contributed in several cases to performance degradation or outages.

Internet and Connectivity Failures

Internet and connectivity failures accounted for 11% of the email outages, which included LAN (Local Area Network) or WAN (Wide Area Network) outages. These connectivity failures prevent users from accessing an otherwise functioning server. Causes of connectivity loss include hub, switch, or router failure as well as broken or damaged cable or fiber from a variety of causes (or accidents) such as construction (backhoe) severing cables and damage during moves or maintenance (human error). In one instance, construction down the street from a surveyed company resulted in the loss of both primary and secondary WAN connections through two separate providers. Infrastructure failures can also occur due to datacenter power outages and causes as mundane as termite infestation.

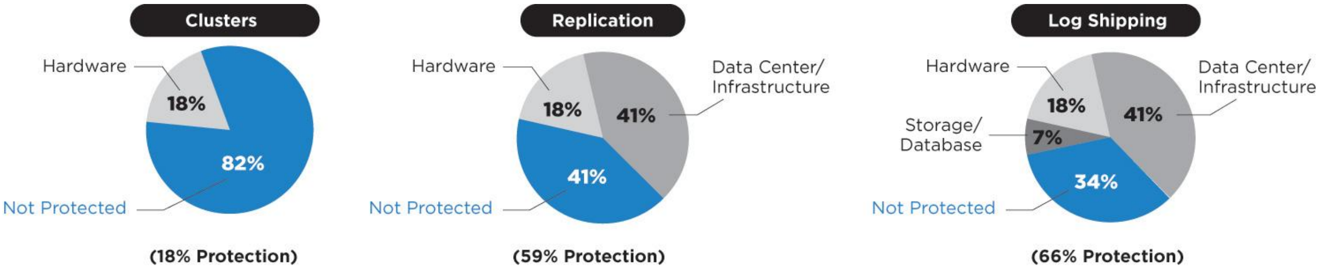
Storage/Database Corruption

Potential downtime due to database corruption is a well-known hazard for mail administrators. With the typical customer having .75TB or more of messaging data, this downtime can be significant. With most of our customers having complex storage systems, operation and maintenance is a challenge. Storage and database corruption includes outages caused by SAN device failure taking out local data stores (technical error), as well as SAN configuration errors (human error) causing data loss windows. When storage systems fail, companies were faced with retention and policy compliance issues, and were forced to undergo costly and time consuming recovery operations from backup tapes.

Common Solutions for Email Availability

The majority of these email outage causes are troubling because they are the most difficult to prevent. Unfortunately the most commonly used solutions to prevent email outages are expensive, complex, and still fail to provide adequate and reliable protection for email. In addition to using backup tape, three of the most common approaches used to avoid downtime are clustering, replication, or by using log shipping. However, each of these solutions only protects your email environment from a fraction of the complete range of causes that can bring down your email system. In addition, these failures typically result in long outages; in fact 78% of email outages last more than four hours.

Figure 3. Clustering, replication, log shipping, and Exchange 2007 do not provide adequate Protection for email



Email Outage Causation – Planned Outages

Survey results showed that planned events account for 24% of email outages in any given 12-month time period. On average, the planned outages last for 35.8 hours. A number of reasons can be sited for planned outages including email platform upgrade or migration, datacenter or office move, planned power outage, system maintenance, required patch management and disaster recovery testing. For example, maintenance windows are necessary to keep servers appropriately tuned or patched. In several instances, customers needed to bring servers down for prolonged maintenance tasks (such as an integrity check on a Microsoft Exchange database), to replace hardware components, to address performance problems, or to preempt impending outages. In some cases theses outages were planned well in advance, in others, they were quickly executed to address problems and potential risks.

Conclusions: despite heavy investment, email still fails

Every day, more and more companies are concluding that email is a mission-critical application worthy of inclusion in a business continuity plan. Generally speaking, organizations' email business continuity and disaster recovery plans fall into two camps: tape backup or replication and mirroring solutions. While tape backup is the most inexpensive way to back up data, tape backup does not provide email continuity – only recovery after a lengthy outage with the potential for lost data.

While traditional replication and mirroring solutions have their place in disaster recovery and business continuity planning, trying to use such solutions for email continuity can prove futile – there is a host of common scenarios for which replication fails to provide high availability.

High Availability Email: Key Points of Failure

Based on the research data collected, there are numerous points of failure with tape backup and traditional replication and mirroring solutions.

1. Failure Point: Replicated Database Corruption

When a corruption occurs in a database store, it can cause a main server to go offline. In most cases, replication software, which transfers data byte-by-byte, will copy the corrupted data to the backup server. In this case, the backup server will be corrupted as well. Typically, corruptions are a slow process of degradation and may require administrators to restore many backup tapes until a tape is found before the corruption.

2. Failure Point: Single Platform Dependency

While most organizations depend on backup email systems, the secondary systems are usually on the same email platform as the primary system. For example, companies that use Exchange Server may have a primary and backup email server running the same version of Microsoft Exchange. This dependency on a single platform creates a point-of-failure where a virus, worm, or bug incapacitate both the primary and backup system simultaneously.

3. Failure Point: SAN Complexity

The very nature of tape backup is just that: 'backup'. An organization uses tape backup generally to backup data – files, databases, applications, etc., which are used/created regularly by the employees of the organization. Tape backup is by far one of the most inexpensive and least complex ways to backup an organization's data. Where tape backup fails as an email continuity and recovery solution, is the fact that it takes anywhere from hours to days to recover a company's data from tape. In the event of a disaster, whether natural, man-made or technological, keeping the lines of communication up and running is critical to recovery. If used as an email backup option, tape backup is too slow to meet reasonable recovery goals.

How Dell Email Management Services (EMS)™ provides email continuity

Hundreds of Chief Information Officers depend on Dell EMS Email Continuity to ensure that email and BlackBerry® services are always available. EMS Email Continuity provides access to a fully integrated standby email system when your primary Microsoft Exchange or Lotus Notes® system fails. EMS is immune to database corruption and Windows viruses, has predictable monthly costs, and can be installed in day.

EMS Email Continuity for Microsoft Exchange

EMS makes Exchange Server outages & maintenance virtually invisible to users

Whenever you have a planned or unplanned outage, EMS kicks in and allows users to continue to send and receive email through Outlook®, a web browser, or via a BlackBerry wireless device virtually without interruption or any change in user behavior. Unlike high availability solutions built upon clusters, replication, log shipping or storage area networks, EMS is not vulnerable to database corruption, Active Directory corruption, configuration errors, Windows® viruses, or Windows malware. As an on-demand service built upon Linux®, EMS is able to offer full interoperability with Microsoft Exchange Server while helping to eliminate all of the dependencies on your primary infrastructure, staff, technology, and mail environment. At a fraction of the cost of on-premise alternatives, EMS is one of the only solutions to effectively eliminate email downtime.

EMS Email Continuity for Exchange Server includes the following features:

- **Effectively Eliminate Email Downtime** – Can be activated in minutes to provide any employee with email & BlackBerry® access during an email outage. EMS helps ensure that email never bounces and that email system outages are never evident to the outside world.

- **Help Eliminate Data Loss** – The data loss windows of tape, replication, log shipping and vaulting are eliminated by restoring lost messages with all forensic information (including time/date stamps, BCC recipients, and read/unread status) back to Exchange after a primary system outage.

- **Outlook Integration Makes It Easy To Use** – Users continue to have access to critical email functionality through Outlook, a web browser, and BlackBerry wireless devices during Exchange outages.

- **Emergency Access to Historical Email** – EMS includes the ability to intelligently synchronize historical email to your standby email system based on your organization's needs. For example, you can provide executives with a full email history, managers with the last five days of email, and other employees with no email history at all in their EMS inbox.

- **Continuity at a Low Cost** – EMS allows administrators to control costs by providing granular control over the amount of email history stored in the back-up system for each user.

- **Exceptional Security** – EMS has been designed with many layers of security to help satisfy the most stringent regulated businesses and the largest enterprises.

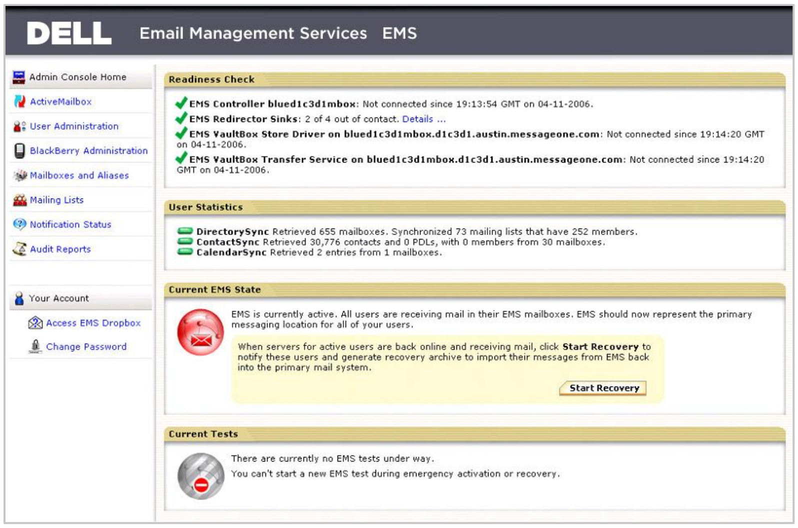
- **Archive Compliance** – EMS is compliant with 3rd-party archiving systems and corporate email retention policies.

- **High Availability for BlackBerry** – During an outage, employees using BlackBerry wireless devices may continue to send and receive messages, even while their Exchange server is completely unavailable.

- **A SaaS-Enabled Solution** – EMS can be fully deployed in a few hours, requires no dedicated staff, and can be easily administered from a single web console for archive, continuity, security, and recovery. EMS is designed for high availability: it's not dependent on your facilities, hardware, software, storage, infrastructure or staff.

EMS is scalable to organizations, can be deployed is as little as a day, automatically synchronizes critical data (contacts, topology, distribution lists, calendars, etc.), and fully integrates with Active Directory and Windows Authentication. EMS compresses, single instances and encrypts email and attachments for secure storage in Dell top-tier disaster recovery datacenters for use in data recovery, end user archiving, comprehensive search, compliance and storage management. Once stored these services are always available regardless of local infrastructure status. EMS has predictable monthly costs, making it a solution that organizations can easily implement regardless of prior investment in email availability solutions. As a fail-over messaging system, EMS provides email as well as BlackBerry access despite any type of problem in your primary system.

Figure 5. Dell EMS Email Continuity



Readiness Check

✓ **EMS Controller blued1c3d1mbox**: Not connected since 19:13:54 GMT on 04-11-2006.
✓ **EMS Redirector Sinks**: 2 of 4 out of contact. Details ...
✓ **EMS VaultBox Store Driver on blued1c3d1mbox.d1c3d1.austin.messageone.com**: Not connected since 19:14:20 GMT on 04-11-2006.
✓ **EMS VaultBox Transfer Service on blued1c3d1mbox.d1c3d1.austin.messageone.com**: Not connected since 19:14:20 GMT on 04-11-2006.

User Statistics

DirectorySync Retrieved 655 mailboxes. Synchronized 73 mailing lists that have 252 members.
ContactSync Retrieved 30,776 contacts and 0 PDLs, with 0 members from 30 mailboxes.
CalendarSync Retrieved 2 entries from 1 mailboxes.

Current EMS State

EMS is currently active. All users are receiving mail in their EMS mailboxes. EMS should now represent the primary messaging location for all of your users.

When servers for active users are back online and receiving mail, click **Start Recovery** to notify these users and generate recovery archive to import their messages from EMS back into the primary mail system.

Current Tests

There are currently no EMS tests under way.

You can't start a new EMS test during emergency activation or recovery.

About Dell IT Management Software as a Service solutions

Dell IT Management Software as a Service (SaaS) solutions simplify the management of your IT environment to get you up and running quickly, with lower deployment costs, fewer hassles, and less time spent on non-strategic tasks.

For more information about solutions for your business or organization, contact your Dell account representative or visit dell.com/services.

Availability varies by country. To learn more, customers and Dell Channel Partners should contact your sales representative for more information.

1 Michael D. Osterman, Osterman Research, June 2008

Trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Specifications are correct at date of publication but are subject to availability or change without notice at any time. Dell and its affiliates cannot be responsible for errors or omissions in typography or photography. Dell's Terms and Conditions of Sales and Service apply and are available on request. Dell service offerings do not affect consumer's statutory rights.