

Why Email Fails

Iron Mountain and MessageOne's Survey of Email Outages

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. The average email user sends 34 emails and receives 99 emails every day, and overall email use is growing 53% per year.

Despite large enterprise investments in replication, mirroring, and tape back up 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.

MessageOne, an Iron Mountain partner, commissioned this research report to understand the frequency, severity, and cause of email outages in North American corporations using Microsoft Exchange, Lotus Notes, and Novell GroupWise. This research shows that enterprise email systems are prone to a variety of potential breakdowns including SAN (Storage Area Network) failures, mis-configuration, losses in network access, database corruption, and viruses. Data from the survey shows that in any given 12-month time period, there is a 75% likelihood of an unplanned email outage and a 14% 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.

SURVEY RESULTS: EMAIL FAILURES BY CAUSE

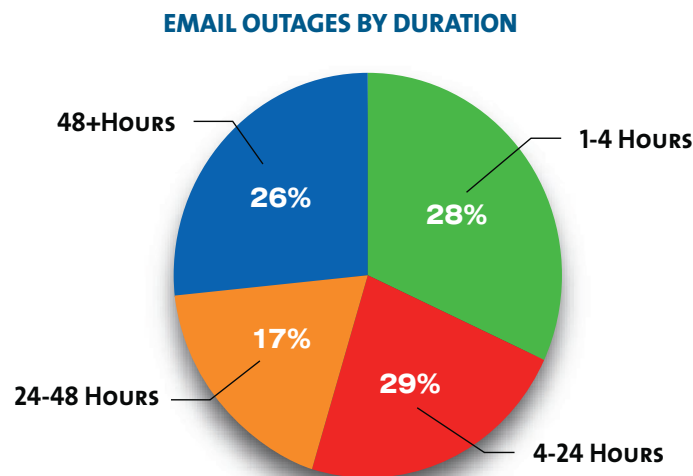
MessageOne, an Iron Mountain partner, recently surveyed its customers on email outages during a recent 30 week period. MessageOne provides hundreds of companies serving over 1,000,000 email users with a highly scalable standby messaging system that can be activated instantly at the customer's request, guaranteeing uninterrupted email services in the event that an organization's primary messaging system becomes unavailable or incapacitated. Companies were surveyed after activation of MessageOne's backup email system, providing timely and reliable reporting on the cause, impact, and duration of email outages.

EMAIL OUTAGE FREQUENCY & DURATION

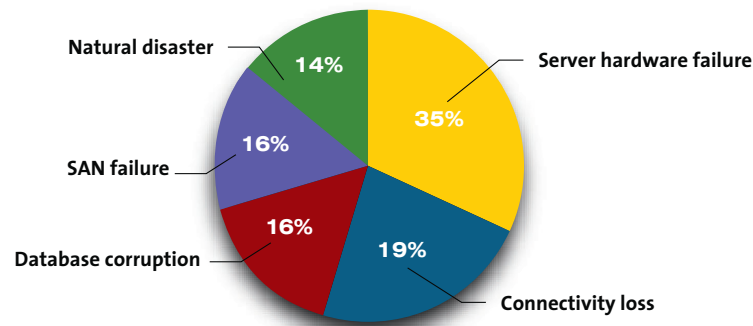
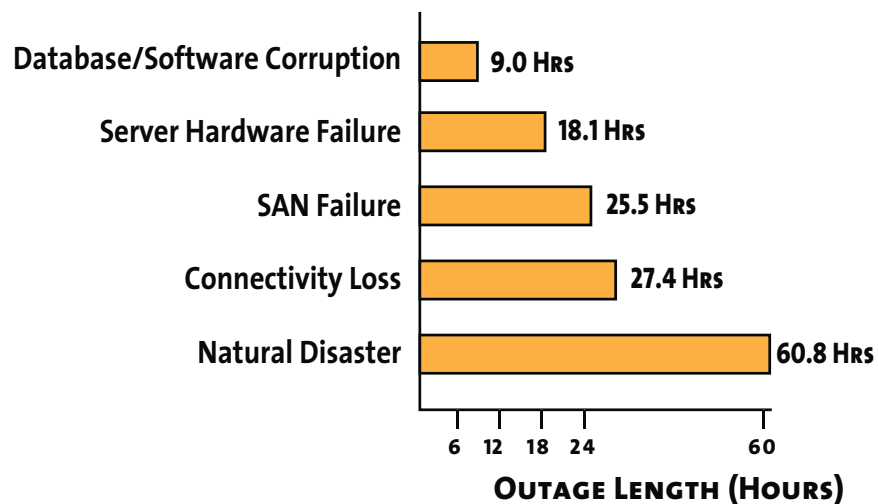
Survey results show that in any given 12-month time period, there is a 75% likelihood of an unplanned email outage and a 14% likelihood of a planned email outage in any given company. The length of email outages in the companies surveyed ranged from a minimum of 2 minutes to a maximum of 120 hours with the average email outage being 32.1 hours long. The largest concentration of outages was between 4 and 24 hours in duration (29%). More than 43% of the outages lasted longer than 24 hours, a length of time that can lead to significant business disruption and damage.

EMAIL OUTAGE CAUSATION - UNPLANNED OUTAGES

A large majority of email outages were caused by unplanned events, most of which were due to technological failures. Of the technological failures, 35% were due to server hardware failures, averaging 18.1 hours in outage duration, 19% were due to connectivity losses, averaging 27.4 hours, 16% were due to SAN failures averaging



25.5 hours, and 16% were due to database corruption averaging 9.0 hours in duration. The majority of these, specifically database corruption and SAN failures, are troubling because they are the most difficult to prevent. Even with expensive mirroring and replication backup solutions, data corruption and SAN failures are often propagated to the mirror or replicated backup server. These failures usually result in long outages as companies resort to incremental tape backups to locate the last backup before the corruption occurred. While natural disasters accounted for only 14% of unplanned email outages, the average downtime due to such disasters was over 60 hours, meaning these can lead to significant impact on businesses.

EMAIL OUTAGES BY CAUSE**DOWNTIME BY FAILURE CAUSE****SAN FAILURES**

Many enterprises have installed a Storage Area Network (SAN) to provide high availability for corporate email services within their headquarter's facilities. SAN hardware, while designed to provide highly available and highly redundant storage for data, adds a significant level of complexity to a messaging infrastructure. Combined with the unique footprint and usage patterns of messaging systems, the design and implementation of SAN infrastructure requires continual optimization to ensure reliable performance.

Mis-configuration of LUNs (Logical Unit Number), out of date drivers, and administration of physical hardware by teams outside of the messaging group were all contributors to SAN-related outages for customers surveyed. In some cases, these errors led to significant data corruption that was replicated to backup email systems.

HARDWARE SERVER FAILURE

A wide array of hardware related failures contributed to outages for customers surveyed. 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.

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. Less well publicized is the risk of downtime associated with Microsoft Active Directory (AD) corruption. Several customers experienced significant system-wide downtime as the result of AD-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.

CONNECTIVITY LOSSES

Connectivity loss includes LAN (Local Area Network) or WAN (Wide Area Network) outages which prevent users from accessing an otherwise functioning server. Causes of loss include hub, switch, or router failure as well as broken or damaged cable or fiber from a variety of causes such as construction (backhoe) and damage during moves or maintenance. 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.

NATURAL DISASTERS

Flooding, hurricanes, power outages, and construction-related network outages accounted for 14% of outages among those surveyed. In one example, a company's top-floor datacenter was unavailable for a week due to flooding. Extreme cold had caused water pipes in the ceiling to burst, leaving their datacenter in four inches of water. In another example, a company had to evacuate their datacenter to exterminate termites.

EMAIL OUTAGE CAUSATION - PLANNED OUTAGES

Survey results showed that planned events account for 14.3% of email outages in any given 12-month time period. On average, the planned outages last for 36.1 hours. A number of reasons can be cited for planned outages including email platform upgrade or migration, data center 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 these 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, organization's 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 amount of 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 back-up 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 Microsoft Exchange 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 can incapacitate both the primary and backup system simultaneously.

3. Failure Point: San Complexity

Complexity makes systems more prone to failure, more difficult to test, and more dependent on key resources that can be deployed on higher value problems. For example, consider a firm that purchased an expensive SAN cluster and configured it to perform Exchange database replication. A truly esoteric mis-configuration caused a complete failure of the SAN and 2 1/2 days without email. Increasingly complex SAN hardware, often used for primary and backup data stores, is becoming a common failure point for enterprise email systems.

4. Failure Point: Dependency On Tape

The very nature of tape backup is just that: 'back up'. An organization uses tape backup generally to back up 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 Iron Mountain's Email Continuity Service Provides Unbreakable Email Continuity

EMAIL CONTINUITY SERVICE OVERVIEW

Email has evolved to become a mission-critical application as essential as electricity or telephone service. In fact, according to a META Group survey, 80% of corporate email users believe that email is far more valuable than telephone for business communications. Today, 90% of corporate communication is driven by email.

Iron Mountain's Email Continuity service is the only affordable solution on the market today that addresses the shortfalls of tape backup and traditional mirroring and replication solutions. The Email Continuity service is a highly-scalable standby messaging and employee notification system that is hosted at world-class disaster recovery facilities equipped with redundant power, servers and internet backbones, and manned 24x7 by expert support staff. The Email Continuity service ensures email continuity 24x7x365 – no matter what.

Features include:

- Email continuity 24x7x365
- 1/20th the cost of traditional replication and high availability solutions
- Makes sure email system outages are never evident to the outside world
- Provides secure email continuity to employees anywhere and any time
- Sends critical notification information to cell phones, BlackBerries, alternate email accounts, etc.
- Can deploy for an entire global enterprise in less than a day
- Is easily tested on a monthly or quarterly basis
- Built on Linux to avoid a single platform point of failure

HOW THE EMAIL CONTINUITY SERVICE WORKS**Prior to Activation**

Prior to activation, critical information about the primary mail system, such as the user directory and employee notification information, is automatically replicated at predefined intervals using Iron Mountain's software that runs in the customer's environment and integrates with multiple back-end systems.

Upon Activation

Upon activation, the Email Continuity service simultaneously performs two actions:

- It broadcasts alerts to the company's employees, notifying them that the Email Continuity service has been activated. Employees will receive these alerts via SMS-to-mobile-phone, RIM BlackBerry (using PIN), text pagers, and alternate email addresses previously provided by the employees.
- It automatically routes all email sent to corporate addresses to the secure, 128-bit SSL the Email Continuity service system hosted at Iron Mountain, readily accessible by employees who have received login instructions via the alerts. Authentication to use the web-based email system can be done with pass phrases, SecureID and other methods that are designed to integrate with the customer's existing security system.

Upon Deactivation

Upon deactivation, once the company's primary mail system has been restored, all emails that were sent or received during the emergency are seamlessly and automatically merged into the company's primary mail system, including all forensic information and timestamps.

©2005 Iron Mountain Incorporated. All rights reserved. Iron Mountain and the design of the mountain are registered trademarks of Iron Mountain Incorporated. All other trademarks and registered trademarks are property of their respective owners.



745 Atlantic Avenue
Boston, Massachusetts 02111
800-888-2774

Iron Mountain operates in major markets worldwide, serving thousands of customers throughout the U.S., Europe, Canada, and Latin America. For more information, visit our Web site at www.ironmountain.com