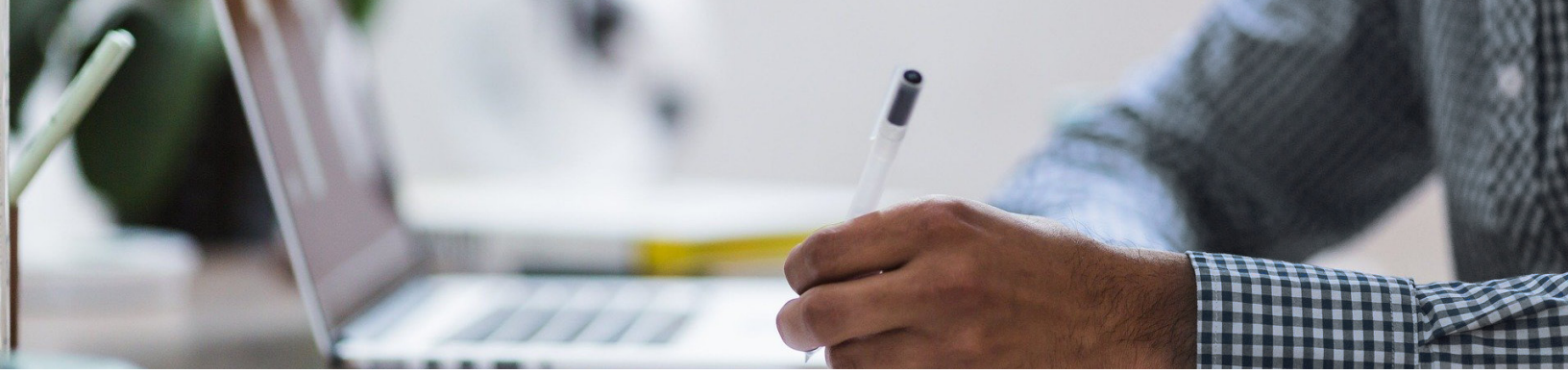
IDEAL EMAIL
WHAT WOULD THAT LOOK LIKE?

bryleysystems®

in partnership with SOPHOS and Kaseya®



Evolve

Email was built for a simpler time – a time when no one had invented phishing or attachments or being compliant digitally. But the world and our needs have changed. So if email for your business could do anything, what would be on your wish list? That's the spirit in which we present Bryley Email Management, created in partnership with Sophos and Kaseya.

Your Email Host and the Truth about Backing-Up and Archiving

Whether your business is using G-Suite, Microsoft 365 or another email server, the fine-print agreements release those providers from liability for anything happening to your email data. The reality is Microsoft, Google, etc. are liable for the infrastructure on which your data resides (i.e. if their data center goes down, they're going to do what they can to get it back and running). They are not answerable for your data, including emails.

You need to treat these cloud servers same as you would if the servers were in your building. Per Kaseya's Alex Courson, "this means [you follow] the 3-2-1 policy, where you have three copies at two locations and one off-site. If you have [all copies of your data] at the same cloud site and Google crashes, you still can't get anything back."

This applies to both backing-up and archiving. These need strategies that

don't rely on the same server that's hosting your email, because nearly eighty percent of organizations that have data in the cloud lose data every twelve months.[1]

Backing-Up and Archiving

Backing-up is the regular copying of your active data — the data is continually evaluated for changes and updated. The purpose of the back-ups is that should disaster strike, a duplicate of your current state has your operation running again quickly.

Bryley's focus is on protecting and preserving its clients' data. The tools Bryley uses to accomplish this goal will change as technologies evolve. Bryley's engineers are continually reevaluating software and hardware to better serve its clients.

In contrast, archiving ensures that your business' records remain secure and retrievable in their preserved, original state for whatever period of time you determine. There is no overwriting of previously saved data. An archive is easy to understand if you think of regulatory requirements. For example a bank needs to retain its transaction records for so many years. But even if your business is not subject to data retention regulations, an employee still may need to locate a PDF attachment from 2017.

Email Continuity in Spite of Mail Server Failures

Bryley Email Management backs up your Microsoft, G-Suite or other server's data. To not slow down your network by moving data across servers during the workday, Bryley's back-up plan runs every night. This means you will have a permanent back-up of a document as it's left at the end of the day. If you find nightly back-ups are not enough, you can supplement with on-demand manual back-ups as often as you would like and can be applied to user accounts or narrowed using granular controls.

Bryley Systems Inc, ITExperts@Bryley.com 978.562.6077

And Bryley's system makes all your email messages — including new messages — available through its web interface. Once your mail server is back online, the Bryley email server re-syncs all your messages with your normal mail client so there are no gaps in service. Bryley Email Management gives you a complete, searchable email archive, including retrieval of emails that have been deleted on your mail server.

Be Confident Mail is Safe, Too

Bryley Email Management creates an encrypted archive (in a Class-A datacenter with a secure and redundant infrastructure) of every message you send and receive. But Bryley Email Management first gives you a series of selectable email security filters. This filter array includes AI Deep Learning (to adapt to spam changes), Bayesian/word statistics, To, Subject and Header field analyses, word pattern analysis, similar vocabulary analysis, SMTP analysis, hyperlink analysis and comparison, contact verification and email format analysis.

Similarly, when sending emails Bryley Email Management is designed to give you confidence in what's being sent by employees — by filtering and encrypting sensitive company and personal data.

Quick Searches of Your Business' Emails

Bryley Email Management makes sure your electronic communications are automatically preserved apart from your mail server, for intelligent discovery, rapid recovery, and continuous access. And there's no new hardware or software to install, all mail is available from any device with a web connection.

Email Encryption That Works

Email was never meant to be secure: The security exposures are on the devices that have the account that sent the email (computer, phone, maybe a second computer), the network (which usually includes a number of switches and routers owned by different companies) where it may be intercepted, the email hosting company's server and the recipients' systems and phones.[2] And if you think it's unlikely someone will get hold of your or your recipients' devices, one of the chief tactics of malware is to search for sensitive data in emails — because emails are low-hanging fruit, i.e. not secure.[3]

One of the ways to address some of these points of exposure, including the switches and routers, the hosting company's server and most email-scanning malware, is encryption.

Encryption turns the content of an email message into random characters to be decoded by the recipient. It's always sounded good, but most implementations have been clunky and cumbersome, and most users feel the answers are more trouble than they're worth. So, the vulnerabilities remain.

Why Encrypt?

Securing information — customer data, employee data, trade secrets — is a best practice for any business. Why take a more lax security approach to email than any other aspect of your IT strategy? And it's often required. For instance, email security is not a choice to meet the compliance rules of GDPR, HIPAA, HITECH, GLBA and FFIEC.

The Key Problem

Typical email encryption works by public keys and private keys. You have your private key. Your public key is given to whomever you choose. When someone wants to send you a secure message, they encrypt it using your public key. Your private key is used to decrypt the message. To send an email to someone else you use your private key to digitally sign the message, so the recipient is sure it's from you.

This can be inconvenient: First setting up each user's encryption keys. And second how do you disseminate your public key? Or get a public key from someone trying to send you a secure email? You can't email or text these keys … securely.

Bryley Email Management Encryption is Different

Bryley's solution makes the reality of secure email attainable for your business, your employees, your vendors and customers. Bryley's approach makes use of a global key repository, that allows you to communicate outbox to inbox with no sender authentication required — an *Encrypt & Send* button is added to your email panes, and without the recipient needing the sender's key. If the recipient is not in the directory, he will receive an email stating you have sent a secure message. The first time he will need to create a password, but thereafter he'll just log in, to decrypt and retrieve your email. If the recipient's email is in the directory (the largest database of its kind), there is no login, he can read the email directly.

What If Someone Emails Sensitive Data Without Clicking *Encrypt & Send*?

Bryley Email Management addresses that: built in is automated message and attachment content-scanning. This means behind the scenes Bryley Email Management employs filters that will encrypt for your business' email senders. You can choose to filter based on content, sender, email domains, email addresses and recipient.

Compliance with governmental and regulatory standards was the basis for many filters: managed lexicons automatically encrypt, reroute, or block email messages containing financial (GLBA) and healthcare (HIPAA) sensitive data. Social security numbers, credit card numbers and medical terminology are part of the managed lexicons that trigger encryption.

Continuous Email Service

Just as a business relies on email to do its work, it needs to make sure its email service is uninterrupted; and it needs to maintain the information in its emails. The fact is there's actually a lot going on under email's hood, including managing data load, the constancy of spam and phishing attempts, unexpected service and power interruptions and unplanned needs to find information within the mass of emails. All these can challenge business managers and employees.

You and your employees shouldn't have to think about what goes on under the hood — email should just always work.

Get a Gateway to Your Mail Server

To achieve always on, always available email Bryley recommends a cloud-hosted email security gateway. An email gateway sits between your company's servers (or Microsft 365 or Gmail account) and people sending you email. It provides continuous on-demand access to your email from any location — even in the event of a network or server outage.

Bryley's email gateway implementation is built with a series of in-depth defenses against unwanted mail ever getting to your staff's email boxes. The service also offers robust outbound processes to ensure viruses are not being unknowingly transmitted, and safeguards against your IP address being blacklisted (blacklisting leads to external servers rejecting your organization's outbound emails).

As an example Microsoft 365 went out November 19, 2019 for about three and a half hours.[4] During that time Bryley Email Management users were able to log into a web client and continue their email communications uninterrupted — without down-time, mail queuing, or sender bounce-back messages. Things happen to computer servers, whether they're on premises or in the cloud; you need to make sure you have a failover like Bryley Email Management.

Unless Your Mail Server's Got Issues, No One Will Know

Bryley Email Management is straightforward to deploy and operates as an unobtrusive gateway to your existing network. Your staff will not be aware of its presence (unless there's a mail server problem and then they can log in to the web client to continue working). Inbound and outbound emails are

typically held on the Bryley mail server for fourteen days; archiving is also available for long-term email storage.

Now That Wasn't So Hard

Business continuity, email back-up, email encryption and email archiving – all pieces of the email puzzle that cannot be neglected today. It protects your company, your customers and vendors, and is part of regulatory compliance. Bryley Email Management's approach is the most user-friendly and intelligent implementation of these business email services. If you would like to discuss securing, archiving and the always-on availability of emailed data, give Bryley a call at 978.562.6077 option 2 or email ITExperts@Bryley.com.

1 https://spanning.com/resources/whitepapers/global-data-protection-survey-report-2016/

2 https://www.digitaltrends.com/computing/can-email-ever-be-secure/

3 https://www.virusbulletin.com/blog/2018/10/emotet-trojan-starts-stealing-full-emails-infected-machines/

4 https://twitter.com/msft365status/status/1196986097856724993?

bryleysystems®

Bryley Systems Inc, ITExperts@Bryley.com 978.562.6077