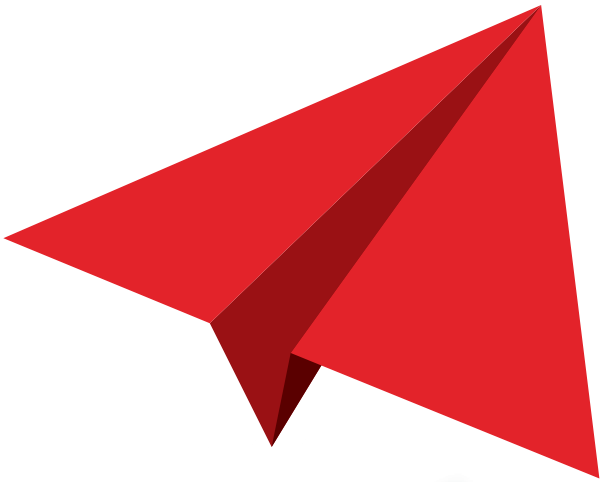
THE STATE OF BUSINESS EMAIL

IN 2014

A WHITE PAPER FOR BUSINESS AND IT DECISION MAKERS

1 INTRODUCTION

EMAIL IS UBIQUITOUS IN TODAY'S BUSINESS WORLD AND EMAIL USAGE AMONG BUSINESS USERS CONTINUES TO RISE.[1]



Yet, there is a widening gap between today's fast-evolving tech environment and standard email technology, the latter of which has not seen any major standard-setting in nearly two decades. Even as this technology gap widens, many business and IT managers remain unaware of either the gap's existence or the serious business risks it poses.

This report discusses the current state of business email in the context of real dangers faced by businesses that rely on email communication. From an institutional loss of privacy and worldwide declines in postal services to increasingly sophisticated cybercriminals, the dangers are relevant, timely, and they demand immediate attention.

2 A LOOK BACK

TO PROPERLY UNDERSTAND THE "STATE OF BUSINESS EMAIL" TODAY, IT IS USEFUL TO UNDERSTAND HOW EMAIL TECHNOLOGY ORIGINATED.

HERE ARE SOME OF THE MILESTONES:

1965

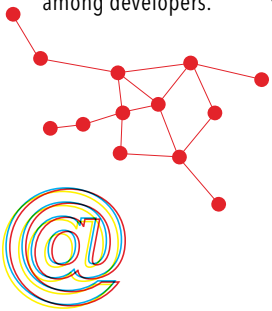
MIT programmers for CTSS (Compatible Time-Sharing System) create an electronic mail system for its users that is possibly the world's first. Note that this system only allowed mail to be sent to/from CTSS users.[2]

1971

Ray Tomlinson uses an existing utility called SNDMSG to send the first email across a network, using the @ sign to separate the user's name and the user's machine.[3]

EARLY 70'S

Email becomes the "killer app" on **ARPANET**, effectively spurring great interest among developers.



1982

SMTP (simple mail transfer protocol) is introduced. SMTP is the widely-adopted standard for electronic mail transmission across Internet Protocol (IP) networks.[4]

SMTP

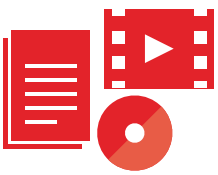
1985

RPost CTO Terence Tomkow is awarded PC Magazine's Editor's Choice award for introducing **"BackMail"**, the first ubiquitous electronic messaging service available using telephone systems

PC EDITORS' CHOICE PCMAG.COM

1993

MIME (multipurpose internet mail extensions) is introduced.[5] Until this point, email message bodies could only contain textual content composed with US-ASCII characters (based on the English alphabet.) With MIME, the message bodies could contain non-English characters and non-textual content such as images or other multimedia content.



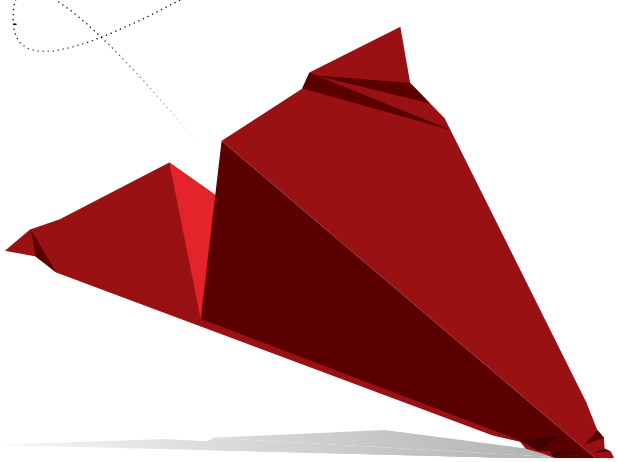
DID YOU KNOW? **DICK PRYOR,** RPOST BOARD MEMBER, WAS HEAD OF THE DEFENSE COMMUNICATIONS AGENCY, WHICH OVERSAW THE ARPANET PROJECT.

One can see from the timeline above that standard email has been developed in a collaborative and iterative process spanning several decades. This type of process is typical of the Internet's foundational technologies, of which HTML and email are two important examples. As a point of contrast, the software development process to create applications using such foundational technologies might take a typical enterprise software company much less time. A company such as Google might be able to come up with a software system using foundational technologies in just a couple of years, because the process involves fewer participants – namely, Google's engineers and management. With a broad foundational technology (such as standard email) that is being co-authored by thousands of contributors around the world and is depended on by countless stakeholders, the pace of collaboration is slowed by a longer feedback cycle and the challenge of having so many "cooks in the kitchen" (and so many patrons in the dining room.)

Another reason for standard email's slow development process is the need for interoperability between networks and computers around the world. Although broad compatibility between networks and computers has been critical to standard email's widespread adoption, it is actually impeding further deployment of email technology standards. This is because any deployment of updated email technology standards requires infrastructure upgrades that many operators are unable or unwilling to make.

One result of standard email's "crippled" development process is that standard email is not yet equipped to deal with recent threats to cybersecurity or certain business requirements such as the need for "email delivery proof." These and other shortcomings will be described later in this report.

ONE RESULT OF STANDARD EMAIL'S "CRIPPLED" DEVELOPMENT PROCESS IS THAT STANDARD EMAIL IS NOT YET EQUIPPED TO DEAL WITH RECENT THREATS TO CYBERSECURITY OR CERTAIN BUSINESS REQUIREMENTS SUCH AS THE NEED FOR "EMAIL DELIVERY PROOF."



3

EMAIL USAGE CONTINUES TO GROW

DESPITE THE FACT THAT STANDARD EMAIL TECHNOLOGY HAS EVOLVED AT A SLOW PLACE, EMAIL USAGE CONTINUES TO RISE THROUGHOUT THE WORLD.

The Radicati Group estimates that the number of email accounts worldwide was 3.9B in 2013[6] , roughly equal to half the people on the planet. This number is expected to grow 5-7% per year for the next few years, across both business and consumer segments.[7] (See Table 1.)

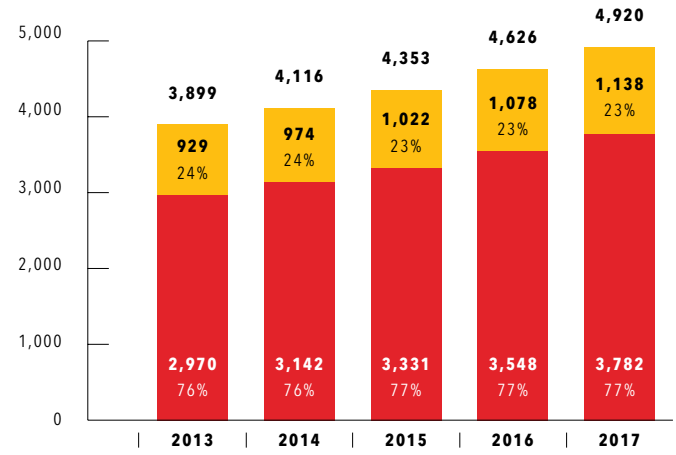
Although the number of consumer email accounts dwarves the number of business email accounts 3 to 1, a significant majority of total emails sent/received falls into the

business category.[8] (See Table 2.) The rise of social media, text and instant messaging in peoples' personal lives surely plays a role in the usage discrepancy, as much of the world's personal messaging has shifted to such platforms. Facebook reports 1.2 billion monthly active users worldwide[9], and mobile messaging provider WhatsApp says it has more than 400 million active users worldwide, for example.[10]

It is important to note that the number of business emails sent worldwide is expected to grow at an average of 7% per year, suggesting that email will continue to be a primary means of business communication well into the future.[11]

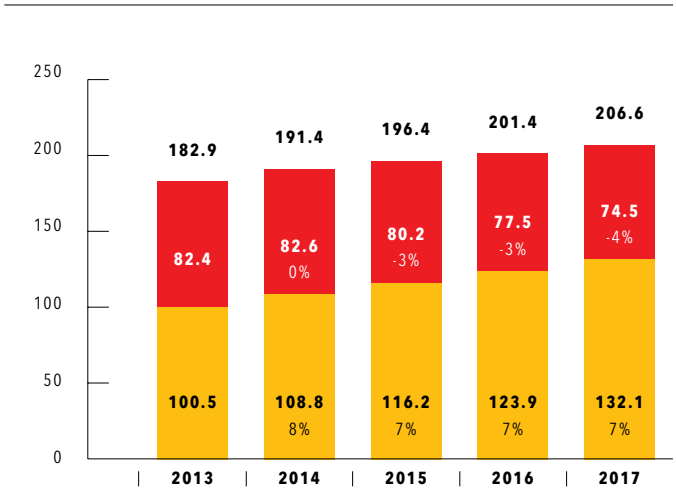
Additionally, research shows that business users are spending more than two hours per day (or approximately ¼ of their work day) reading and writing emails, on average.[12] Despite this huge time investment in using email technology, many of these "heavy users" are not aware of the limitations posed by standard email. These limitations are described in the following section.

BUSINESS VS. CONSUMER EMAIL ACCOUNTS
(M), 2013-2017



Source: The Radicati Group. (April 2013). Email Statistics Report, 2013-2017, Executive Summary.

WORLDWIDE EMAIL TRAFFIC
(B), 2013-2017



Source: The Radicati Group. (April 2013). Email Statistics Report, 2013-2017, Executive Summary.

4 — WEAKNESSES OF STANDARD EMAIL

BECAUSE EMAIL HAS BECOME A PRIMARY MEDIUM FOR BUSINESS COMMUNICATION, IT IS CRUCIAL FOR IT DECISION MAKERS, RISK MANAGERS AND OTHER BUSINESS MANAGERS TO UNDERSTAND STANDARD EMAIL'S LIMITATIONS.

Standard email has often been criticized for having deep-rooted security vulnerabilities and other shortcomings due to the dual challenges of "slow iterative development" and "need for cross-platform compatibility."

HERE IS A SUMMARY OF THE PRIMARY CRITICISMS:

1. Email messages have to go through intermediate computers before reaching their destination, meaning it is relatively easy for others to intercept and read messages.

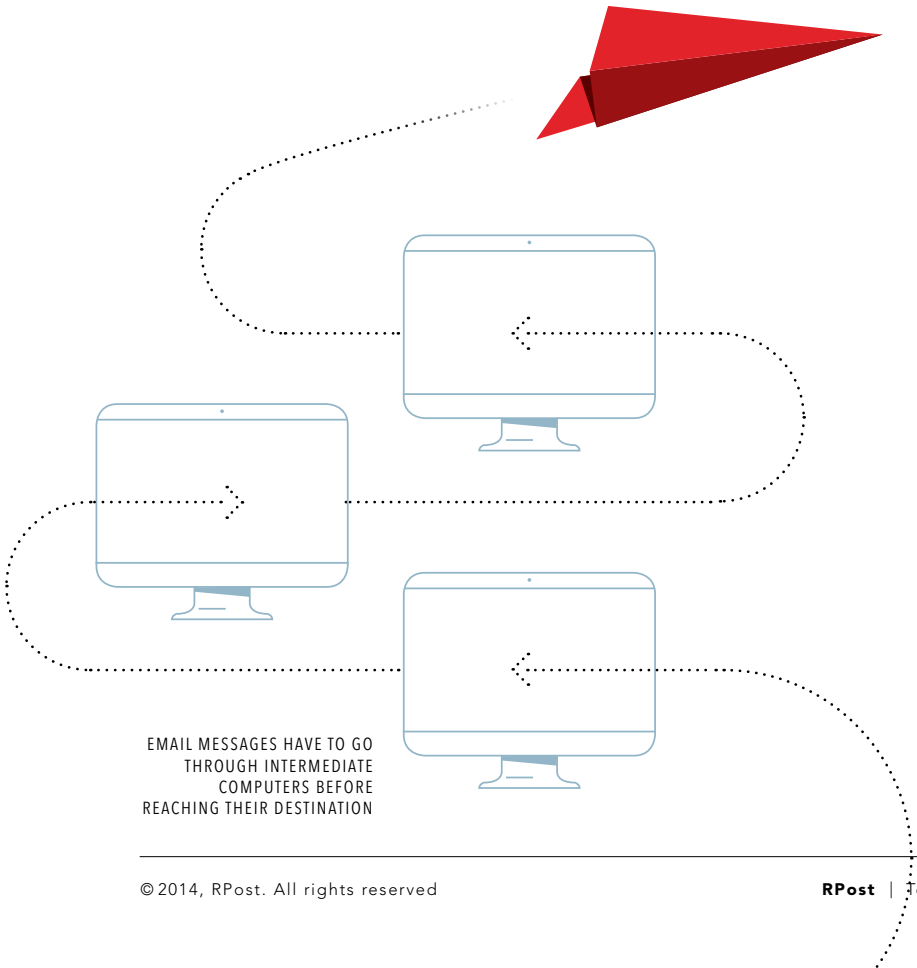
2. Standard email messages are encoded in a plain text format that offers no protection against unintended access.

3. Many Internet Service Providers (ISP) store copies of email messages on their mail servers before they are delivered or retrieved. The backups of these can remain for up to several months on their server, despite deletion from the mailbox.

4. Standard email providers and 3rd party mail clients do not provide the proof of email delivery many business users require.

1 Email messages have to go through intermediate computers before reaching their destination, meaning it is relatively easy for others to intercept and read messages.

SMTP's mail processing model requires an outbound email message to be relayed to a minimum of four different computer servers (mail service agent, mail transport agent, mail exchanger, and mail delivery agent) across any number of networks prior to successful delivery. In practice, the number of "stops" can be even greater, depending on the route selected by the MTA or the sender or recipient's use of services such as spam filtering. The multitude of "stops" on an email's way to the email recipient means increased susceptibility to hackers and "packet sniffing" technology that can peer into unencrypted emails and record both sender/recipient information as well as message content.



EMAIL MESSAGES HAVE TO GO THROUGH INTERMEDIATE COMPUTERS BEFORE REACHING THEIR DESTINATION

2 Standard email messages are encoded in a plain text format that offers no protection against unintended access

Standard email messages that one sends by clicking the standard "Send" button in Microsoft Outlook or Gmail (or other email software), are encoded in a plain text format that offers zero protection from packet sniffing and other means of intercepting emails. Though the merits of email encryption have long been clear to those who understand email's mail processing model, email encryption has not yet been deployed into many email providers' systems or even leading email client software – despite the availability of encryption technologies such as Open PGP, S/MIME, TLS and others.

The omission of encryption technology from global email deployment is due to the fact that international standard-setting bodies for email technology have not identified an encryption standard that satisfies the disparate groups of stakeholder users and companies throughout the world. Part of the challenge stems from the importance of maintaining interoperability among the thousands of email systems around the world, many of which are

decades old and may not support recent encryption standards. In the meantime (prior to deployment of a global email encryption standard,) it is important for businesses to provide users with an email encryption service that they can easily use to protect sensitive information both in transit and at rest.

3 Many Internet Service Providers (ISP) store copies of email messages on their mail servers before they are delivered or retrieved. The backups of these can remain for up to several months on their server, despite deletion from the mailbox.

The risk of losing information at rest (stored on the sender/recipient's device or on a mail server) is different from that posed by hackers/spies using packet sniffers to intercept email messages. In the case of emails at rest, a sufficiently motivated party could gain access to the sender/recipient's computer or the ISP's mail server and steal any stored email messages. In light of this, businesses need to protect their email even when it is at rest; this can be achieved using an email encryption service that supports "message-level encryption," which protects emails at rest AND during transit. RPost's email encryption service, for example, uses an encrypted "PDF wrapper" to provide email users with message-level email encryption for their emails and any attachments.

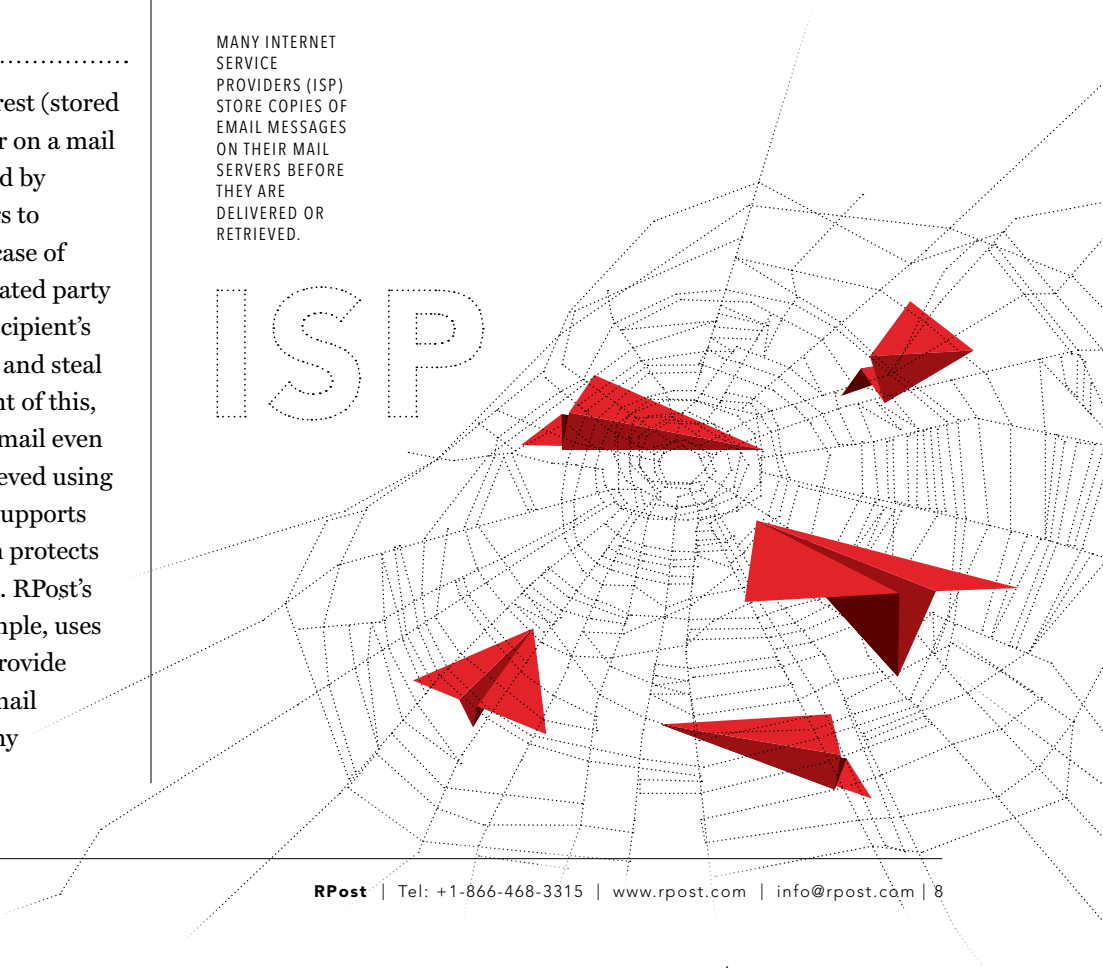
4 Standard email providers and 3rd party mail clients do not provide the proof of email delivery many business users require.

Regardless of industry, business users need proof of message delivery from time to time. For example, trial lawyers need proof they've served opposing counsel by email when opposing counsel claims non-receipt. Manufacturers may want to retain proof that they've sent change orders to suppliers, or distributors notice of pricing changes. Insurance brokers can send customers updates on plan coverage or notices of coverage changes by email while retaining proof that such information was delivered, which protects them from liability in case of a later claim of non-receipt.

DID YOU KNOW?

BY USING RPOST'S REGISTERED EMAIL® SERVICE, BUSINESS USERS CAN SEND IMPORTANT CORRESPONDENCE BY EMAIL AND AUTOMATICALLY OBTAIN COURT-ADMISSIBLE PROOF OF EMAIL DELIVERY.

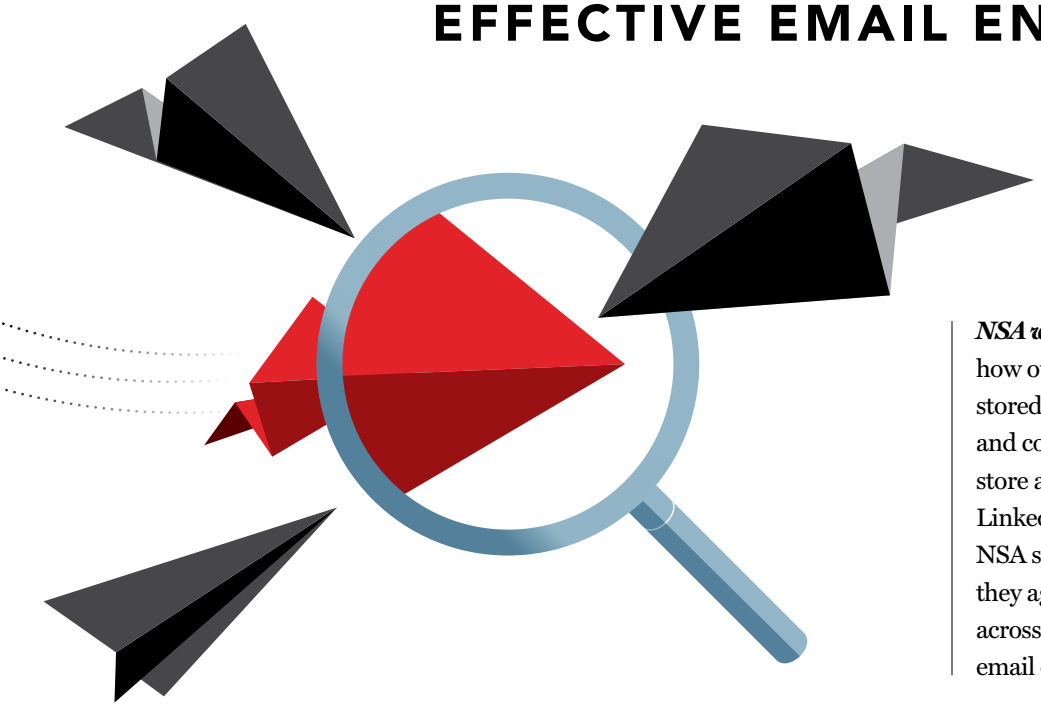
MANY INTERNET SERVICE PROVIDERS (ISP) STORE COPIES OF EMAIL MESSAGES ON THEIR MAIL SERVERS BEFORE THEY ARE DELIVERED OR RETRIEVED.



5

IMPORTANT TRENDS AFFECTING BUSINESS EMAIL

NSA WHISTLEBLOWER UNDERSCORES THE NEED FOR EFFECTIVE EMAIL ENCRYPTION



NSA whistleblower Edward Snowden exposed how our digital identities are being captured, stored, analyzed, and categorized by the NSA and companies that publicly state that they store and analyze your data (Facebook, Linkedin, Google email, etc.) The power of the NSA system, according to Snowden, is that they aggregate your digital communications across telephone, Internet, mobile app, and email data.

With regards to email, email encryption can keep your email content private. As The Guardian reported on June 17, 2013, Snowden said:[13]

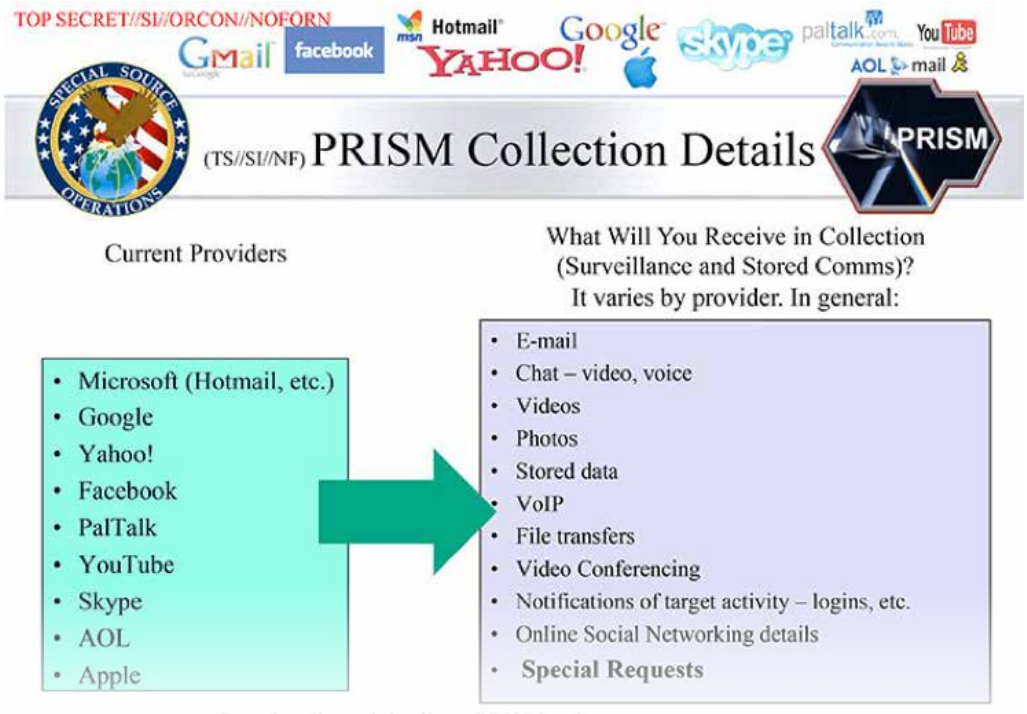
"ENCRYPTION WORKS. PROPERLY IMPLEMENTED STRONG CRYPTO SYSTEMS ARE ONE OF THE FEW THINGS THAT YOU CAN RELY ON."

Edward Snowden

The problem, however, is that standard email is not sent in an encrypted format. Users that value email privacy, whether for legal compliance or for privacy reasons, need to use a third party email encryption service to ensure that their messages and any attachments are secure.

Yet, many email encryption services commercially available today are not particularly effective against either government surveillance or hacker attacks. Many leading email encryption providers use a "store and forward" system, whereby sensitive emails are stored on the service provider's servers where they can be accessed by the recipient via web log-in. Such a collection of sensitive information, in many cases containing personal information such as home addresses and credit card numbers, is essentially a treasure trove of information that government spy agencies and hackers can target by subpoena, written request or illicit means.

Only a few email encryption systems keep email content in an encrypted format (such as RPost's encrypted PDF wrapper) from endpoint to endpoint, even when the messages are at rest. Such a system employs what is called as "message-level encryption" to ensure that even if the government or a hacker successfully gets to your emails, they won't be able to access the information within (without somehow breaking your encryption.)



A SLIDE FROM A LEAKED TOP-SECRET PRESENTATION ON PRISM, A CLASSIFIED NSA SURVEILLANCE PROGRAM. THE PRESENTATION WAS DATED APRIL 2013.

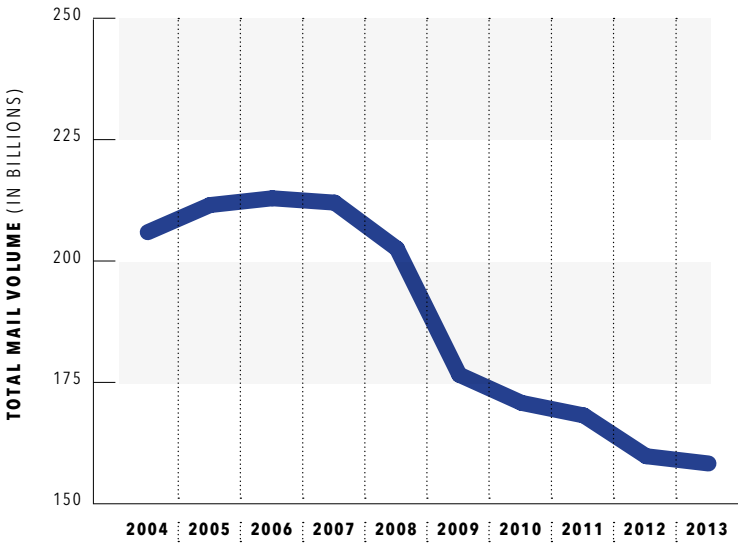
Global Economic Downturn and the Decline of Postal Services

The global economic downturn that started in 2008 may be reversing in global equity markets and economic statistics, but the cost-cutting business strategies the recession brought on are here to stay. One key strategy for cutting costs that businesses adopted is "going paperless." From 2006 to 2009, North American paper consumption declined by 24%.[14] Businesses have realized that electronic communication is both less costly and faster than paper-based communication and are aggressively shifting much of their communication to "paperless."

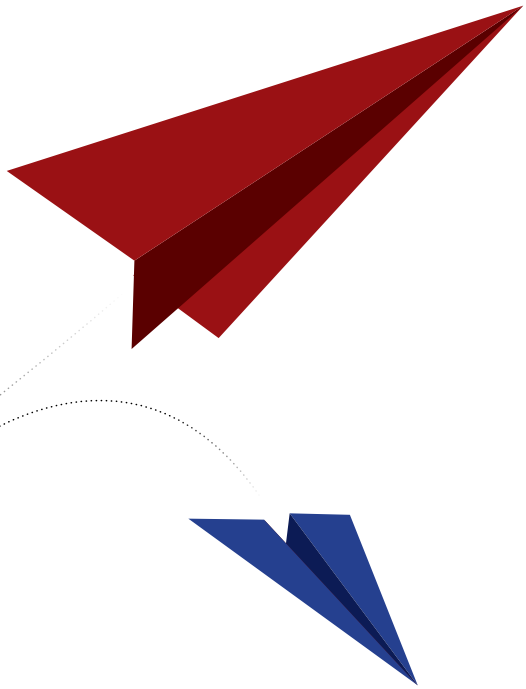
One consequence of the shift is that postal carriers throughout the world are left with a bloated postal infrastructure and rapidly declining mail volumes to support that infrastructure. This has caused postal carriers to experience dramatic financial losses (such as USPS's $15.9B loss in 2012[15]), downsizing, and sometimes even outright elimination of postal delivery options that have existed for decades (such as Canada Post's elimination of home delivery.[16]) For businesses that rely on postal services, this presents a bleak outlook: higher postal prices and a lower quality of service.

Yet, for those businesses that have already migrated to electronic or "paperless" communication or plan to do so, challenges still remain. High-value correspondence traditionally sent by private courier or certified first class mail cannot be entrusted to standard email, because standard email is insecure and lacks proof of email delivery. Only RPost's Registered Email® service bridges the security gap (using email encryption) and offers the legal proof of email delivery many users require.

UNITED STATES POSTAL SERVICE (USPS)



Source: USPS.com, Postal Facts 2014



Heightened Enforcement of Data Privacy Laws

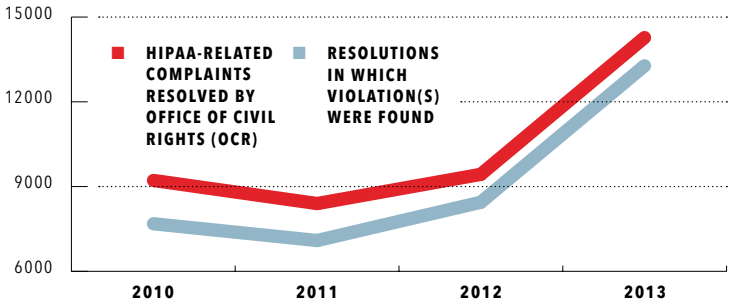
The continued prevalence of hacker attacks, malware and other threats to digital privacy has reinforced the importance of data privacy laws such as HIPAA (Health Insurance Portability and Accountability Act). In 2013, the U.S. Department of Health and Human Services expanded HIPAA with a final Omnibus rule that "greatly enhances a patient's privacy protections, provides individuals new rights to their health information, and strengthens the government's ability to enforce the law" by:[17]

1. Broadening HIPAA so that it also applies to business associates of companies that receive protected health information (PHI)
2. Increasing the penalties for non-compliance according to negligence, with a maximum fine of $1.5 million per violation[18]
3. Strengthening the Health Information Technology for Economic and Clinical Health (HITECH) Breach Notification requirements by clarifying when breaches of unsecured health information must be reported to HHS
4. Affording the individual greater control over their protected health information

The final deadline for full HIPAA compliance was September 23, 2013.[19]

As a consequence of this final rule, any healthcare provider or business associate that handles PHI must use an email encryption service when emailing PHI. Because of the heightened HIPAA enforcement, it is also important for businesses to retain proof that PHI was sent in an encrypted format. Such proof is particularly valuable in the event of downstream data breaches, as businesses need to prove that any data breach did not happen on their watch.

HIPAA ENFORCEMENT ON THE RISE



Source: HHS.gov

CIVIL MONETARY PENALTIES

TIER	PENALTY
Covered entity or individual did not know (and by excercising reasonable diligence would not have known) the act was a HIPAA violation.	$100–$50,000 for each violation, up to a maximum of $1.5 million for identical provisions during a calendar year.
The HIPAA violation had a reasonable cause and was not a due to willful neglect.	$1,000–$50,000 for each violation, up to a maximum of $1.5 million for identical provisions during a calendar year.
The HIPAA violation was due to willful neglect but the violation was corrected within the required time period.	$10,000–$50,000 for each violation, up to a maximum of $1.5 million for identical provisions during a calendar year.
The HIPAA violation was due to willful neglect and was not corrected.	$50,000 or more for each violation, up to a maximum of $1.5 million for identical provisions during a calendar year.

DID YOU KNOW?

ONLY **RPOST'S REGISTERED EMAIL® SERVICE** PROVIDES AUTOMATIC PROOF OF ENCRYPTED EMAIL DELIVERY

Proliferation of Hacks, Malware & Spam

There are a number of sophisticated hacker and malware tactics that have been effective in the last couple of years. Here are a few of the more effective tactics involving email messages:

EMAIL SPOOFING

A technique used by hackers and spammers to fake their identity when sending emails. This is particularly easy to do because standard email protocols do not authenticate sender identity.

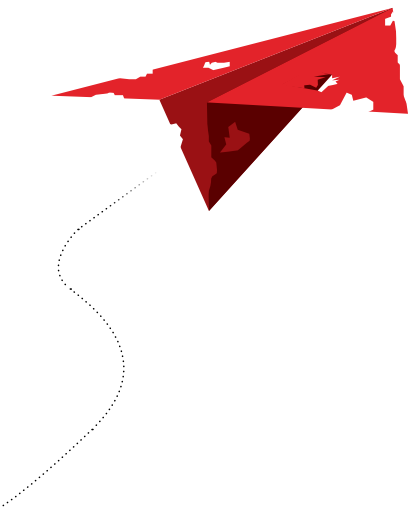
MALWARE

Malware refers to any type of malicious code that attempts to disrupt computer operation, gather sensitive information, or gain access to computer private systems. It is estimated that malicious attachments were contained in 3.9% of all emails in Q3 of 2013. [20]

PHISHING

A phishing attack is one where the perpetuator attempts to trick victims into providing valuable info such as credit card numbers or bank login information, in many cases by sending victims to a webpage that looks like a legitimate webpage (such as an online banking login page.) These attacks often come in the form of an official-looking "spoofed" email from the perpetuator.

In 2013, there was a prevalence of fake news mailings – about the birth of the royal baby or the FBI hunt for Edward Snowden, for example – that linked to a compromised website that redirected to another webpage containing a popular exploit kit called Blackhole[21] . According to Kaspersky, "Once users reach the website, Blackhole starts searching for vulnerabilities in their software. If it finds any, it downloads several malicious programs, including Trojan spyware designed to steal personal data from victim machines."



Spam

In the early days of email, spam (or unsolicited bulk mail) was not expected to become a significant threat. Therefore, email servers were programmed without any mechanism by which to authenticate sender identity – allowing senders to easily fake their identities (by forging information in message headers, for example.) This vulnerability led to a massive surge in spam, despite the threat of prosecution and fines imposed by laws such as the U.S.' CAN-SPAM Act of 2003. It was estimated that about 90% of all emails sent in 2010 were spam.[22]

Though recent data suggests spam is on the decline, in part due to more stringent mail transfer agent (MTA) requirements, spam continues to be a problem. Kaspersky estimates that 68% of all email messages sent in Q3 of 2013 were spam.[23] With all the inbox clutter, two email service upgrades have become very important to business email users: spam filters and Registered Email® messages.

SPAM FILTERS

Mostly implemented by IT administrators, spam filters are spam detecting algorithms that score message metadata and content to separate spam email from legitimate email. Note that spam filters are not completely reliable, and it is common for some unsolicited bulk email to still get through the filters.

REGISTERED EMAIL® MESSAGES

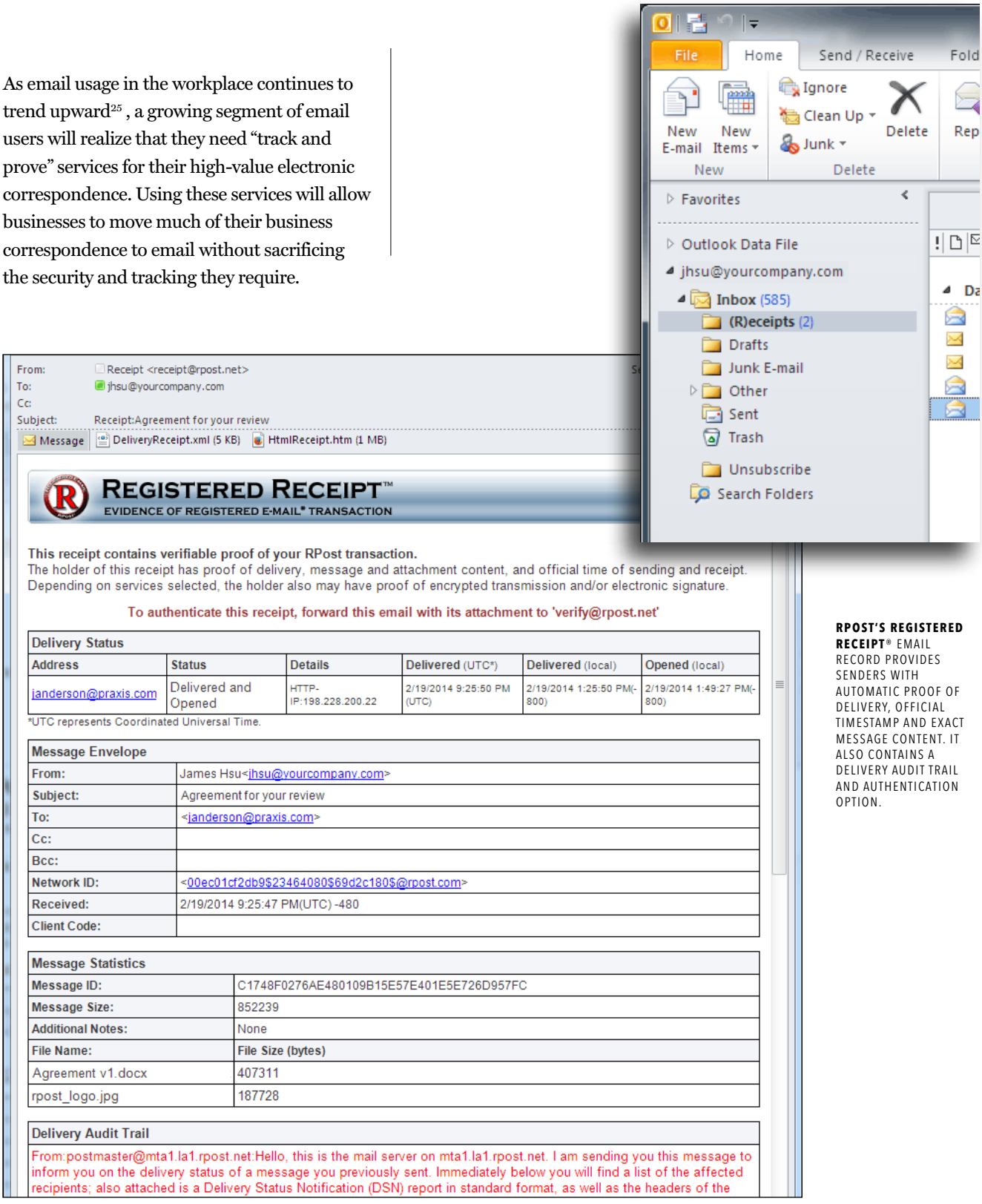
Registered Email technology allows email senders to elevate the importance of their email messages by affixing them with special "Registered Email" markings, including disclosure to the recipient that the sender will receive proof of delivery. Many users of the Registered Email service have noted that recipients are more responsive to Registered Email messages than to standard email. [24]

6 A LOOK AHEAD

GOING FORWARD, INCREASINGLY SOPHISTICATED CYBER THREATS AND A RENEWED COMMITMENT TO DATA PRIVACY WILL DRIVE MANY BUSINESSES TO ADDRESS A WIDENING GAP BETWEEN STANDARD EMAIL AND THEIR SECURITY/PRIVACY NEEDS.

Many will turn to third party email encryption services, while some will cease to send sensitive information via email. International standards-setting bodies for email will continue to discuss different encryption standards, but deployment of a global standard will continue to be hindered by interoperability challenges posed by old technology in use around the world.

As email usage in the workplace continues to trend upward[25], a growing segment of email users will realize that they need "track and prove" services for their high-value electronic correspondence. Using these services will allow businesses to move much of their business correspondence to email without sacrificing the security and tracking they require.



RPOST'S REGISTERED RECEIPT® EMAIL RECORD PROVIDES SENDERS WITH AUTOMATIC PROOF OF DELIVERY, OFFICIAL TIMESTAMP AND EXACT MESSAGE CONTENT. IT ALSO CONTAINS A DELIVERY AUDIT TRAIL AND AUTHENTICATION OPTION.

ABOUT RPOST

RPOST HAS SET THE GLOBAL STANDARD FOR EMAIL DELIVERY PROOF, ENCRYPTION, AND E-SIGNATURES WITH ITS PATENTED REGISTERED EMAIL® TECHNOLOGY.

RPost services enable email users to track, prove, sign, encrypt, and collaborate across desktop, mobile, and web platforms. RPost services speed contract execution, increase data privacy and compliance, and reduce risk with court-admissible records.

Founded in 2000, RPost operates from six global business centers, is in use in countries throughout the world, within governments and Fortune Global 500 companies, and has been endorsed and marketed by influential bar associations throughout the United States. Winner of the World Mail Award for Security, RPost holds 50+ patents worldwide. For more information, please visit www.rpost.com.

6033 West Century Blvd.
Ste 1278
Los Angeles, CA 90045

1-866-468-3315
www.rpost.com
sales@rpost.com

REFERENCES

1. The Radicati Group. (April 2013). Email Statistics Report, 2013-2017, Executive Summary. Retrieved from The Radicati Group's database.

2. Van Vleck, Tom. (Feb 1, 2001). The History of Electronic Mail. Retrieved from http://www.multicians.org/thvv/mail-history.html.

3. Tomlinson, Ray. The First Email. Openmap.bbn.com. Retrieved from http://openmap.bbn.com/~tomlinso/ray/firstemailframe.html on 2/12/2014.

4. Postel, J.B. (Aug 1982). Simple Mail Transfer Protocol. RFC 821.

5. Borenstein, N. Freed, N. (Sep 1993). MIME (Multipurpose Internet Mail Extensions) Part One: Mechanisms for Specifying and Describing the Format of Internet Message Bodies. RFC 1521.

6. The Radicati Group. (April 2013). Email Statistics Report, 2013-2017, Executive Summary. Retrieved from The Radicati Group's database.

7. Ibid

8. Ibid

9. Facebook. (Jan 29, 2014). Facebook Reports Fourth Quarter and Full Year 2013 Results. Retrieved from http://investor.fb.com/releasedetail.cfm?ReleaseID=821954

10. Ripley, Charles. (Dec 19, 2013). WhatsApp Pushes Past 400 Million Monthly Users. PC World. Retrieved from http://www.pcworld.com/article/2081851/whatsapp-pushes-past-400-million-monthly-users.html.

11. The Radicati Group. (April 2013). Email Statistics Report, 2013-2017, Executive Summary. Retrieved from The Radicati Group's database.

12. The Radicati Group. (Aug 2013). Business User Survey – 2013. Retrieved from The Radicati Group's database.

13. Glenn Greenwald. (Jun 17, 2013). Edward Snowden: NSA Whistleblower answers reader questions. The Guardian. Retrieved from http://www.theguardian.com/world/2013/jun/17/edward-snowden-nsa-files-whistleblower on 2/12/2014.

14. Environmental Paper Network. (2011). State of the Paper Industry, 2011. Retrieved from http://environmentalpaper.org/our-resources/2011-state-of-the-paper-industry/ on 2/7/2014.

15. USPS. (Nov 15, 2012). Postal Service $15.9 Billion Loss Highlights Urgent Need for Legislative Reform in Congressional Lame Duck Session. Retrieved from http://about.usps.com/news/national-releases/2012/pr12_131.htm.

16. The Economist. (Dec 14, 2013). The postman won't ring at all. Retrieved from http://www.economist.com/blogs/americasview/2013/12/canada-post-ends-home-delivery.

17. The U.S. Department of Health and Human Resources. (Jan 17, 2013). New rule protects patient privacy, secures health information. Retrieved from http://www.hhs.gov/news/

18. Ibid

19. (Jan 25, 2013). Federal Register, Vol. 78, No. 17. Retrieved from http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf on 2/12/2014.

20. Kaspersky. (2013). Spam Statistics Report Q3-2013. Retrieved from http://usa.kaspersky.com/internet-security-center/threats/spam-statistics-report-q3-2013.

21. Ibid

22. MAAWG. (Mar 2010). 2010 MAAWG Email Security Awareness and Usage Report, Messing Anti-Abuse Working Group/Ipsos Public Affairs. Retrieved from http://www.maawg.org/sites/maawg/files/news/2010_MAAWG-Consumer_Survey.pdf

23. Kaspersky. (2013). Spam Statistics Report Q3-2013. Retrieved from http://usa.kaspersky.com/internet-security-center/threats/spam-statistics-report-q3-2013.

24. RPost. (Jan 2014). 2013 End User Survey. Retrieved from RPost survey database.

25. The Radicati Group. (April 2013). Email Statistics Report, 2013-2017, Executive Summary. Retrieved from The Radicati Group's database.