Ensuring E-mail Security

Some services are available that ensure encryption of messages even while sitting on servers.

By Michael Menapace

This is the inaugural column by the ARIAS•U.S. Technology Committee. It is our hope that this recurring feature can provide practical and helpful information to the reinsurance community.

At the ARIAS•U.S. Spring 2017 Conference, arbitrators were invited to attend a workshop intended to help arbitrators and others in the ARIAS•U.S. community with limited IT support staff understand the potential vulnerabilities of sending and receiving confidential information via e-mail and to adopt some simple and low-cost baseline practices to keep the information secure.

This workshop and these materials are an extension of the draft *Guidance for Data Security in Arbitrations* that is currently being considered by ARIAS•U.S.

Basic Information and Background

The *Guidance for Data Security* uses the term "confidential information" to refer to various types of information that can be exchanged in the course of an arbitration, including the subsets of personally identifiable information ("PII"), protected (or personal) health information ("PHI"), and sensitive or proprietary business information. While various laws and regulations require different levels of confidentiality treatment depending on the subsets describes above, the *Guidance* treats the subsets similarly so that implementing information security measures can be done efficiently.

For some years, insurance and reinsurance companies have been aware of information security risks and safeguards and have invested considerable amounts of time and money to implement robust information security procedures, protocols, and practices. Their efforts are routinely examined and revised. Likewise, law firms have been implementing information security practices and, in most cases, have systems in place to protect confidential information while at rest and in motion. For example, most companies and many firms have e-mail systems that automatically encrypt outgoing messages, while encrypted messages can be automatically unencrypted by the receiving party for seamless and secure communication.

A weak link in the process is when the receiving party uses an e-mail system that cannot, or does not, accept encrypted messages. In this scenario, the e-mail must be sent in an unencrypted format or the sender must make other arrangements (as discussed below) to get the information to the recipient.

Regulators from a host of agencies have been requiring insurers to address this potential weak link as part of the wider trend of considering companies' use and sharing of information with third-party service providers, vendors, and other business partners. For example, the New York Department of Financial Services cyber security regulation requires (among other things) insurance companies to assess the risk that their vendors pose to the security of certain information, require those vendors to implement reasonable safeguards, assume the risk those vendors pose to information security, and attest in writing that they (the insurers) have undertaken these steps. As an example, it has become commonplace for insurers to require law firms to submit their written data security plan and allow the insurers to perform random audits of firms' practices and technology.

Requiring vendors to use a secure e-mail system is a minimum requirement on which companies will insist,

even for their smallest vendors and service providers.

Commonly Used Free E-mail Providers

Gmail, Yahoo, and Hotmail e-mail accounts are ubiquitous and free to the user.

Advertising space is sold. To do this, the service providers "read" your e-mails to target advertisements to you. *See* Terms of Service.

In addition, the providers share this information with their sister companies. Gmail = Google, YouTube, etc. Hotmail = Microsoft.

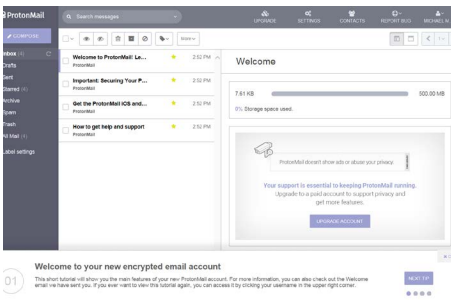
Some of these services advertise that your e-mails are encrypted. But that is generally true only while the e-mails are in transit, not while resting on the providers' servers, and only when you are communicating with other accounts with the same provider.

Once a bad actor gets into the provider's system, it is relatively simple to copy communications from large swaths of users (e.g., as in recent Yahoo revelations).

These are risky systems to use if you want your communications to remain confidential.

Encrypted E-mail Providers

A better alternative to the free e-mail services discussed above are the free and high-security options. Many people find it convenient to maintain two accounts, rather than trying to move everything from an existing account to a new account. Alternatively, many people will use a newly created account for matters moving forward and leave prior files in the existing account.



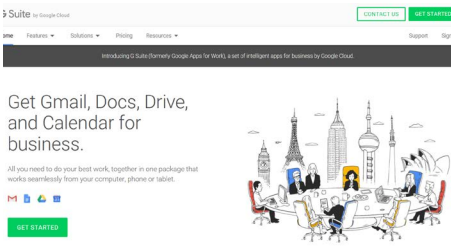
Among the free secure e-mail providers are Proton Mail and Tutanota. These services are free up to certain space limitations. Inexpensive upgrades are available to increase space, allow for multiple users on the same account, or customize your domain name. For example, you could make your name JoeTheArbitrator@BestArbitratorEver.com. ProtonMail (www.ProtonMail.com) provides 500 MB free storage, with a $4 per month upgrade. Tutanota (www.Tutanota.com) provides 1 GB free, with a $1.20 per month upgrade.

When using these services, your e-mails are encrypted while in transit and while at rest. The providers cannot unencrypt even if they want to do so—something that people operating in some places around the world find advantageous or that journalists prefer so they can correspond with whistleblowers or other sources.

Both providers have mobile apps for your smartphone or tablet device, and they use a familiar-looking interface so the transition to a new e-mail program is relatively simple. For example, here is the inbox for a ProtonMail account. You can see the familiar folders on the left, the list of e-mail messages in the center, and the reading pane on the right.

At the Spring 2017 Conference workshops, people asked how these "free" services make money if they do not sell advertisements. They derive revenue primarily from people who upgrade their accounts. In addition, there is an option for users to donate to help support the service, similar to how people donate to Wikipedia or other public interest crowdfunded platforms.

Upgrading to G Suite



If you use Gmail and do not want to use a secure e-mail provider such as ProtonMail, Google offers the option to upgrade free Gmail accounts to G Suite (formerly Google Apps for Work and Google Apps for Your Domain).

Unlike the free, consumer-facing services, G Suite users do not see advertisements, and information and data in G Suite accounts do not get used for advertising purposes. G Suite administrators can fine-tune security and privacy settings.

Data is encrypted while resting in Google's data centers, but Google has the encryption keys, unlike the high-security options discussed above. This means that if faced with a subpoena or other court order, Google could access your G Suite account.

To upgrade from Gmail, you need to sign up for G Suite, select a domain name, customize your domain name settings, and move your data. The interface looks and works very much like standard Gmail. (Neither Hotmail nor Yahoo have the ability to upgrade to a similar product like G Suite.)

If you have questions on the use of secure e-mail, please reach out to a member of the Technology Committee or, if in the course of an arbitration, one of the parties. It is in everyone's interest that information be kept secure and confidential.