Data Encryption Done Right

May 23, 2018

RIAs are increasingly aware that electronic communication with clients, custodians and vendors needs to be locked down. Whether they are taking the right steps to encrypt data is another story.

Other Articles: Cybersecurity For Small RIAs • Securities America Advisors Now Able To Text Clients
Trending Articles: Red Flags That Can Trigger An IRS Audit Of Client Tax Returns • Giant Recruiting Loans By LPL, Others Questioned By Consultants
Advisors and their clients communicate electronically in at least one of the following ways: through e-mail, portals or, increasingly, via text. After considering the options for securing these communications, advisors may be surprised to learn what actually offers the most protection.

Texting

Texting appeals to many for convenient and instant communication, but texts between RIAs and clients have many cybersecurity downsides. Texts are difficult to monitor, and though they can be encrypted, it’s challenging. Any files shared and uploaded in texts are unsecure and may be vulnerable.

Advisors who thrive on texting, then, should consider doing it through a platform such as Skype’s that offers more secure communications (as long as both parties use its service). But the current lack of security options is just one of a host of reasons RIAs should forgo texting with clients altogether.

One of the biggest reasons is the Securities and Exchange Commission’s Office of Compliance Inspections and Examinations (OCIE), which focuses on communications, including texts. If an advisor is going to respond to inbound texts, all sides of those exchanges must be encrypted and archived and should have data loss prevention enforcement applied. An encrypted texting service may be able to handle this, but the archiving costs can be expensive.

Client Portals

It is quite common for RIAs to use secure portals for sharing personal information that can be used to identify clients and other sensitive data. Client portals have been in existence for a while, and many offer good encryption methodologies while the information is both at rest and in transit.

Portals rely on one of two kinds of security: authentication and obscurity (when secrecy is built into the design). Think of it as the difference between being given a link and logging on to a website. Authentication uses encryption keys, or passwords, which are given to clients for their documents only, and it offers more protection and is preferred over obscurity, which relies on complicated URLs that can be hacked more easily.

A portal can also be used as a permanent storage vault for important documents. And though a portal requires clients to maintain another set of log-on credentials, RIAs tend to find them relatively easy to use.

While client portals offer more security than texting, they have several drawbacks. The lack of security on the client's side can leave the portal vulnerable to breaches. In fact, portals typically leave copies of files on individual computers, which may be unencrypted, meaning the data can potentially be accessed by intruders.

Also, most portals store files without scanning them, which means they could download viruses. Meanwhile, auto syncing tools, which automatically synchronize files to a vault as well as to a client's own computer and vice versa, bypass the security measures in place on the devices and servers. This means that they directly send and receive files, including those with viruses or malware.

RIAs can work around this by also using a vault that scans uploaded documents for viruses.

Simply storing identifying client personal information on a public vault can also expose that information to a hack. But by adding an additional level of encryption to the file, the level of security increases at the file level, as well as at the vault level and on the client's personal computing devices.

Though the cost of portals is fairly inexpensive, most do not offer the full archiving capabilities necessary to show adherence with the OCIE's archiving and data loss prevention recommendations. Very few portals offer users the ability to back up to previous versions, so RIAs still need some type of archiving solution that allows them to retrieve earlier versions of files.

E-mail

E-mail is the most commonly used form of client communication, so it is also the most exposed to hacks and data breaches. But with the right data encryption tools in place, it is actually e-mail that can be the most secure way to transmit and archive data and a client's personal information.

Surprised? Don't be. A cottage industry has grown up around securing e-mail, which means that encrypting, sending, receiving and archiving it are at least as secure as using a client portal, and maybe more so.

Some RIAs have said it can be difficult to know when to send encrypted e-mails, and the process has historically been cumbersome and inconvenient. But things have changed for the better. Today, some software can scan e-mail contents before sending them to determine whether encryption is even necessary. Users could also simply encrypt all their e-mails.

There are also seamless solutions offered by firms that allow encrypted e-mail to land directly in a client's inbox, while others require clients to access encrypted e-mails through a portal. Either way, clients can view the e-mail securely, even on mobile devices. RIAs can also add a level of security to encrypted e-mails and attachments so they can be in "view only" mode—in other words, the e-mail cannot be forwarded, copied, saved or printed.

E-mail archiving is also relatively inexpensive next to texting and client portals. The cost can vary widely, though, landing anywhere from $20 to $6 to archive a mailbox, so it pays for RIAs to shop around.

Other Articles: Cybersecurity For Small RIAs • Securities America Advisors Now Able To Text Clients
Trending Articles: Red Flags That Can Trigger An IRS Audit Of Client Tax Returns • Giant Recruiting Loans By LPL, Others Questioned By Consultants
When it comes to data encryption, the hard part for most advisors is making the leap from convenience to security. Since the OCIE has made data encryption a necessity, for RIAs it is not a question of "if" but "how" to best protect a client's personal data and other sensitive information. Advisors who dismiss the real possibility of client and firm data hacks are making a misstep that could have significant ramifications.

Wes Stillman is the chief executive officer of RightSize Solutions, a provider of cybersecurity and technology management services for wealth management firms. He can be reached at wnstillman@rightsize-solutions.com.