Speaking to Clients About

Cybersecurity

Securities America
Your business growth expert.

SPEAKING TO CLIENTS ABOUT CYBERSECURITY

Create Your Message

The first step is to create a client message the same way you would for any other service you provide. Educating clients on cybersecurity is yet another way you provide value. This reinforces the trust they put in you to help them achieve their financial goals. Here are a few things to consider:

Main Points

The main points of your message should:

- ❒ Acknowledge the cyberthreats affecting consumers every day and that you take these threats very seriously.
- ❒ Articulate your policies and explain how your team is addressing concerns.
- ❒ Educate clients on best practices to minimize cybersecurity risks.

Value Proposition

Incorporate your approach to cybersecurity into your value proposition statement showing you take the issue seriously. You have a professional approach to meet cyberthreats, so make it part of the value you deliver in your services.

Prepare for Discussion

Make sure you are prepared to have a discussion with anyone, including clients and auditors, about your actions to meet cybersecurity threats. Like any communication, you must know your audience, so your delivery will vary based on who you are communicating with and the communication channel.

For example, when speaking with clients highlight processes you have implemented to combat cybersecurity threats and focus on "why" you are doing them. Address at a high level the concerns you perceive in the cyber landscape and your actions to help protect their financial future.

When speaking with an auditor or a client who is also a small business owner, be more detailed in your delivery. Focus on "how" you are addressing cybersecurity concerns. As always, it is important to know with whom you are speaking. DO NOT over-communicate your procedures, unless officially requested by a regulator or auditor, as you could be providing a fraudster with information they could use to exploit your defenses.

Reinforce Your Commitment

Just like with other services you provide it is important to remind clients what you offer. Reinforce your commitment to maintaining a secure practice by incorporating cybersecurity best practices and educational content in newsletters and other communications. Educational articles are commonly available through a number of third-party marketing providers. Reinforcing your commitment to cybersecurity protection demonstrates the value you provide to your clients.

Create your message by:

- ❒ Adding to your Value Proposition
- ❒ Prepare for discussion
- ❒ Reinforce your commitment

Meetings and Seminars

Now that you have created a strong cybersecurity message, it is time to deliver it. You can start by sharing some information in a newsletter or email blast, but have an official conversation with your clients as part of an annual or semi-annual meeting. For prospective clients, include your cybersecurity promise when communicating your services. Carve out as much time as you need to deliver your message, but consider the following:

- ❒ Create the framework for your discussion by citing recent news articles and statistics – show clients and prospects that we face cybersecurity threats every day.
- ❒ Clearly communicate that you take cybersecurity very seriously, and you have a plan in place to minimize the risks of operating a business in this modern age of technology. Iterate that your job is to ensure they fulfill their financial dreams, and the risk associated with cybersecurity is yet another threat to their plan. Reinforce their trust in you by providing this value in your business approach.
- ❒ Provide your clients with best practices (examples provided on page 14).
- ❒ Document when you had the discussion with your client and note what you shared.

In addition, consider hosting cybersecurity seminars with clients and prospects. Securities America has created a pre-approved client seminar that focuses on identity theft. If you feel competent in this area, create your own or seek a qualified third party to provide the educational content. The FBI is a great resource to contact for speakers and content. Seminars are the perfect way to educate, generate engagement and reinforce your commitment to clients and prospects alike.

Conduct an official meeting, as part of an annual or semi-annual review, or a seminar with your clients about the topic of cybersecurity.

Provide Best Practices

Here are some cybersecurity best practices you can share with your clients.

- ❒ Back up data. Recommend that clients backup their data using either a cloud-based solution or external hard drive. This can help minimize disruption caused by a ransomware attack.
- ❒ Be cautious with downloads. Preach caution when downloading from unfamiliar sources, websites and links provided in emails from unknown addresses. In fact, ceasing this sort of activity will greatly reduce their risk of accidentally downloading a virus or other form of malware.
- ❒ Do NOT click website ads. Instruct your clients to avoid clicking on website ads, even those appearing to be from reputable sources. The website administrators may not properly vet ads on their site, which may contain malicious code and malware. If the ad is from a reputable site, just go directly to the site from a new browser window. Additionally, suggest using an ad blocker and anti-tracking software.
- ❒ Do NOT overshare on social media. People have a tendency to overshare on social media to the point that cybercriminals take note. Spear-phishing attacks and targeted spam email are more effective when personalized using the information found on social media. For example, a cybercriminal will use social media to identify and impersonate a person's friend or family member. Then they send a personalized email containing a virus or phishing request while claiming they have a new email address[6]. Advise your clients to be cautious about what they post to social media because the information is generally freely available for all to see.
- ❒ Use security software. Similar to your own policies and procedures, recommend your clients use and frequently update antivirus and antispyware software. Many internet service providers allow residential subscribers access to free subscriptions of popular antivirus and internet protection tools.
- ❒ Update software and operating system. Recommend clients aggressively update other software (like Java and Adobe) and their operating systems whenever a patch or new version is available.
- ❒ Implement home network security. Recommend your clients activate password protection on their home Wi-Fi network and they have their network/computer firewalls on. Also, suggest they turn off their computers when not in use – this limits their exposure in case of a breached network.
- ❒ Create strong passwords. Everyone, including clients, should create strong passwords and use different passwords for different sites. Strong passwords make it more difficult for cybercriminals to hack and different passwords for different sites reduces exposure of login credentials for a compromised site.
- ❒ Use precaution on public networks. Free public Wi-Fi is convenient, but everyone should take precaution when using it. It is important to verify with an establishment the name of the free Wi-Fi network and to turn off file sharing on the device accessing that network. Also, do not accept updates to applications and software while accessing a public network because the traffic may not be encrypted. Plugins are available that will force secure connections whenever possible, such as HTTPS Everywhere. A useful article with best practices pertaining to safe public network use is available at www.cnet.com.
- ❒ Preach what you practice. For small-business-owner clients help them out by providing details on the cybersecurity policies and procedures you have implemented in your business. You can even point them to the framework and small business resources in this guide.