# PREPARING FOR **CYBER RISKS**

By Marty Bicknell, CEO & president, Mariner Wealth Advisors

While in recent years we've continually shared insights regarding the importance of cybersecurity, I've become aware of an increase in fraudsters hacking email accounts and attempting to initiate wire transfers along with an increase in ransomware attacks. All of these potential threats are why Mariner Wealth Advisors has developed internal control processes and trained its advisory teams to be vigilant in identifying these situations.

So, how did we advance our cybersecurity measures?

### Forming a Cybersecurity Team

Getting the right people in place was the first step. We established a team that included associates from IT, compliance and members of the executive team to help identify the risks, what needed to be protected, what we already had in place and what, if any, gaps we had. Moreover, this team was tasked with creating the overall program and risk management solution that included internal controls and policies and processes we would eventually put into place.

### Auditing Current Processes

The team began by reviewing our existing policies and programs in comparison to the current regulatory requirements and recommended security

standards. From a technology perspective, the team also looked at our technology infrastructure, such as hardware, software, data and user management. Finally, they reviewed access points, networks and physical security for all of our locations. This review process took into consideration the tools we use to run the business and interact with our clients, because we know that protecting our clients means equipping our associates when it comes to mitigating cybersecurity threats.

### Documenting Updates

After we completed our review, we shifted our focus to establishing the policies, procedures and best practices we wanted our associates to follow each day. This resulted in updates to our employee handbook, Business Continuity Plan, vendor risk management process and cybersecurity programs to manage the process and train our associates.

### Introducing Tools for Associates

Along with these new resources, we also introduced several new tools to help our associates manage data more securely. For example, it can be difficult to securely manage usernames and passwords which are used for so many access points. To address that issue, we introduced a secure password protection software that not only stores them in an encrypted environment, but it also provides every user their own Security Dashboard that alerts them to potential risks

and provides on-demand training on how to improve their online security. Additionally, we introduced an email surveillance system that will hold suspicious emails in a secure environment, allowing our associates to review them before acceptance.

We've even adopted new services to enhance our employee benefits programs. These include legal services and ID monitoring programs for associates and family members. Our goal is that not only will our associates develop new habits at the office but will also use them in their personal lives.

## Providing Associate Training

As we introduced these new resources, it became very import to turn our attention toward training our associates so they could develop new habits. We accomplished this by conducting mandatory training on how to recognize potential security threats. Each of these training sessions is like a "fire-drill," demonstrating what could happen and how to respond. The overall goal is to keep physical and data security top of mind. With repetition, it's allowed our associates to become better prepared.

## Educating Our Clients

When educating our clients about cyber threats, we approached it in two ways. First, we distribute articles like these.

- Protect Yourself: Cyber Fraud Alert
- Cybersecurity: 10 Tips to Protect Yourself and Your Personal Data

The second approach we used to educate our clients is demonstrating how types of cyber risk tools and best practices could be used in their daily lives. For example, we leverage a secure email system and a secure online vault for sharing important documents. The email system allows files to be encrypted during transmission and then can be opened by a client through a specialized portal. The online vault is also secured and can only be accessed through the client portal, which uses a dual authentication process.

Preparing our associates and clients for cyber risk also included developing a Business Continuity Plan. Little did we know how much that would be put to the test until this year. With the COVID-19 pandemic in full swing, our advisors operated remotely according to our plan, and we navigated our client communications just as it was designed. While our clients certainly miss meeting with us in person, we feel reassured that our preparation worked.

## Seven Best Practices to Follow

To say it ends there would be a misstatement because, with cyber risks, continued vigilance and preparation are ongoing. So, I'll conclude by sharing some good habits our data security team recently shared as we continue to work from remote locations around the country:

1. Have a password for every computer.
2. Don't share it or write it down on a post-it-note!
3. Keep your computer up to date.
4. Keep your business devices separate from your personal devices whenever possible.
5. Lock your computer – yes, even at home, especially if you have little ones.
6. Check the security of your home network.
7. Don't use public networks.

Finally, follow your Business Continuity Plan, and if you need help managing your cyber risks, get help.