Your Six-Point Spring Cleaning Cybersecurity Checklist

April 28, 2021

For me, spring is a season to clean up and make room for new growth and opportunities. After hibernating through the coronavirus pandemic, the onset of spring seems more significant in 2021 than in years past.

As I've noted in more detail in Financial Planning, now is a great time for RIAs to revisit their cybersecurity policies to ensure that their protocols make sense in today's environment.

No time to read the full article? No problem. I've summarized my six-point checklist for RIAs below to help you think through how to get your cybersecurity program on track and up to regulatory par.

> **✓ Are my cybersecurity compliance policies updated for remote work?**
> *Consider:* You may now have the technology to support remote work, but are your cybersecurity policies and protocols updated to protect client and firm data? Have you tested these policies to know whether they'll pass regulatory muster?
>
> **✓ Are my fintech and tech stacks integrated?**
> *Consider:* Better management and integration of your fintech and tech stacks result in better cybersecurity and data protection. True integration is achieved through a hybrid approach to technology management.
>
> **✓ Does my firm's 2021 tech budget account for potential risk as well as growth?**
> *Consider:* Typically, 20 to 25 percent of the RIA's tech spending goes to the tech stack, with the remainder allocated for the fintech stack. In 2021, we're advising most firms to plan for a five to 10 percent increase in spending on the tech stack, compared to last year.
>
> **✓ Are we consciously communicating on cybersecurity with clients?**
> *Consider:* Make sure you reach out to clients to update them on the cybersecurity upgrades you've made to keep their information secure and protected.
>
> **✓ Does our firm foster a culture of cybersecurity?**
> *Consider:* A culture of cybersecurity starts at the top. Revise your tech policies regularly to adjust for changes in the business and require everyone at the firm to review and sign the updated documents annually. Share headlines on data breaches with employees, with reminders on why certain policies are in place, and celebrate the firm's cybersecurity successes.

✔ Do you really know what's going with your vendors?
Consider: You need to understand how your tech vendors store and protect their data, so if there's ever an issue, you can communicate with your clients with some assurances.

After reviewing this checklist, if you've decided that a thorough cybersecurity house-cleaning is in order, don't delay – make it a priority to understand where you need to fill in the gaps to protect against potentially devastating data breaches. And then get ready to roll into this next season of opportunity.