FINANCIAL ADVISOR

If You Hate Your Compliance Officer, Wait Until You Meet The CISO

November 2, 2023 • Mark Hurley, Allan Starkie

Most wealth managers use their internal IT staff to handle cybersecurity. This is somewhat analogous to asking knee surgeons to perform spinal surgery. Although they are highly trained physicians and experienced in cutting bone, it is a whole new world when dealing with spines.

Similarly, IT professionals are experts in making technology work. Preventing it from being breached is an entirely different expertise. It requires years of training and experience that most IT professionals lack.

This is the sixth article in a series that examines wealth management firm cybersecurity. It looks at the issue of what talent industry participants will need, what they will cost and how they can get them.

As detailed in earlier article in this series, how wealth managers manage cybersecurity risks soon will change. A combination of regulatory and financial liability is going to force firms to operate from a cybersecurity perspective much more like large accounting and law firms with closed systems that can be accessed only by company-owned and managed devices.

To make this work, industry participants are going to need to recruit staff with the necessary expertise. Certainly, most firms will work with vendors to provide technology and consulting services. However, cybersecurity is not static, and each firm has its own vulnerabilities. Cybercriminals continually innovate new tactics to which firms will have to adjust to over time. This, in turn, will force industry participants to both stay abreast of new threats and constantly update their defenses. Doing so is almost impossible without internal expertise.

Moreover, as described in an earlier article in this series, new regulations likely to be approved later this fall by the SEC place the responsibility for having adequate cybersecurity policies and procedures squarely on wealth management firm management. Failing to take the necessary steps will be considered a violation of fiduciary duties and trying to blame a vendor after a breach is unlikely to be well received.

Further, the Commission left open the issue of whether to require industry participants to appoint a chief information security officer or CISO to oversee their organization's cybersecurity just as it previously mandated that all firms appoint a chief compliance officer to oversee compliance. Our view is that even if it elects not to do so immediately, it is almost a certainty that the SEC will revisit the issue and institute this requirement as greater numbers of wealth managers are breached.

Unfortunately, finding and recruiting a CISO will be both challenging and expensive for the foreseeable future. Globally the demand for qualified cybersecurity professionals currently exceeds its supply by more than 3.4 million people and in the U.S. alone there are 700,000

unfilled positions. The shortage of such talent is so bad that even public company boards are struggling to find members with the requisite cybersecurity expertise.

Moreover, retaining such staff is also potentially challenging due to the associated stress of being responsible for protecting an organization from cyberattacks originating from across the globe. Indeed, a recent survey of senior cybersecurity professionals found that 73% had experienced burnout in the past 12 months.

As with any shortage of talent, their cost has skyrocketed. The median salary for cybersecurity staff is now more than $237,000 per year. In certain markets such as Los Angeles, it exceeds $260,000 per year. It also important to keep in mind that this is just salary alone. When budgeting for such positions, wealth managers should assume that, in addition to benefits, the employee would receive a bonus of about 20% of their salary.

However, this is just for cybersecurity staff. CISOs are management positions that oversee an organization's cybersecurity structure and vendors, tactics and strategies, processes and procedures and deal with the SEC should the firm be breached, while at the same time ensuring that the firm can still function. Additionally, they often are in the unenviable position of having to say no to extremely annoyed and aggravated people. And the worst offenders when it comes to not following firm cybersecurity procedures and policies are invariably senior management. Understandably, the cost of recruiting and retaining such individuals will be significantly higher.

The obvious questions are where and how wealth managers are going to be able to recruit both CISOs and cybersecurity staff. It is unlikely that recent college graduates will have the necessary skills, expertise and judgment. Instead, the needed individuals will likely be sourced as lateral hires from larger organizations. Perhaps someone who is currently a number two or three cybersecurity executive at a larger company will find appealing the opportunity to be the CISO for small to midsized businesses such are wealth managers.

Another obvious question concerns how many industry participants will be able to afford the steep incremental costs of additional technology and staffing, especially given that the median size of RIAs is only $415 million of assets under management. We believe that many smaller firms will need to affiliate in some fashion with larger service platforms, such as Kestra, Carson and Dynasty.

To be sure, they will remain independent wealth managers. However, a partnership with these kinds of organizations will allow them to effectively share the necessary resources and immense costs with many other industry participants.

A combination of cybersecurity threats and new regulatory demands soon will complicate the lives of every wealth manager. The earlier that these organizations can find and recruit the right people to help address both, the less painful will be the upcoming changes.

Mark Hurley is CEO of Digital Privacy and Protection (DPP). Allan Starkie is managing partner of Knightsbridge Advisors.