VOLUME 32, NUMBER 12 DECEMBER 2022

Edited/Published for leading financial professionals - www.bobveres.com

Data Security and Cyber Compliance

Synopsis: ***Here's a quick rundown of the best ways to protect your tech stack and client data from bad actors.***

Takeaways: ***Get an independent assessment of whatever your IT provider has installed. You can access a cyber manual that maps the various cyber obligations directly to the regulatory requirements, and start the process of becoming a Digital Asset Fiduciary.***

As you could probably suss out from the headline, this article is about cybersecurity, which is admittedly not the most exciting topic in financial history. (Tax-aware decumulation of retirement portfolios seems downright sexy in comparison.) That may be why you don't see a lot of articles about it.

This is a mistake. My friend and colleague Joel Bruckenstein, the expert on our fintech landscape, has been in my ear about the growing cyber risks to financial planners, and how too many planners seem to be addressing these risks haphazardly. The idea of a major hack of sensitive client data, possibly at multiple firms in a short period of time, and the ensuing awful publicity splashed all over the profession, keeps him awake at night.

Personally, I can't imagine why any unscrupulous people with excellent computer skills would ever want to hack into the computer systems of a group of professionals who collectively have the ability to wire billions of dollars of client money to their anonymous accounts in the Cayman Islands. And I'm sure if that happened, those clients would totally understand how inconvenient it would have been to install rigorous safety protocols.

But purely to satisfy my own curiosity (and definitely not to get Joel off my back), I decided to explore the topic, specifically to identify the most effective protocols currently on the market and where to find them.

Joel's main point in these conversations is that there needs to be cyber separation of duties in place, not unlike how, in another area, we have advisors managing client assets while custodians make sure those assets are where they belong.

In the cyber realm, that separation is rare. Most firms employ somebody to install various software protections (for a pretty comprehensive article on the tech options, go here: *https://www.advisorperspectives.com/articles/2022/07/11/the-state-of-the-art-in-remote-technology-access*)--and that might be a local IT person or an industry-specific provider like Visory or Smarsh. But should they rely on that same IT company to verify that the right tech is in place? (*Sure; everything's great! We installed it, didn't we?*) Joel's point is that there should be a second vendor involved, who looks over what the IT person installed, compares it with best practices, does an audit of the firm's internal processes, and certifies (or not) that the firm's tech stack and clients are appropriately protected.

So who does that kind of work? I recently talked with Brian Edelman, of FCI (*https://fcicyber.com*), a cyber service provider that has been around since 1995. Edelman's credentials include a Certificate in Cybersecurity Risk Management from Harvard University, but I think his most important credential is that he knows the advisory business inside and out. He was raised in a household where his mother was an advisor, but as he worked with clients, he felt himself drawn more to the privacy aspect of the advisor-client relationship than to managing assets.

"We had wealthy people sharing a lot of information with us that nobody else knew," Edelman says today, "and there wasn't a lot of thought given to how to protect it. I looked around," he adds, "and I realized that financial advisors were collecting very private information from their clients, but not taking security very seriously."

Today, FCI works with somewhere between 2,000 and 3,000 advisors, largely congregated among larger firms. In a typical relationship, he finds that the advisory firm's education level on cyber issues is not high. "Advisors mostly focus on how to take care of their clients, and they rely on others for IT issues," Edelman says. "In many cases, they'll install antivirus and leave it at that. But cyber is something you have to keep your eye on all the time. It's a discipline all in itself."

And, he says, echoing Bruckenstein, every firm needs to have an independent security assessment—what Edelman prefers to call 'cybersecurity scanning.'

How does it work? Edelman says that the basic protocols used by the most sophisticated industry cyber experts were created by an Obama-era government program called the Institute of Standards & Technology, which continues to issue and update its Cybersecurity Framework. "They bring in all the best minds," Edelman explains, "and they say, *how do we protect the industries in America?* And they develop the guidelines for an industry to adopt."

Advisory firms have to be able to identify all of their cyber assets-- and be able to detect, in real time any attempted or successful attacks.

The most basic translation into lay terms is that all firms have to be able to identify all of their cyber assets—all the computers that the firm is using, all the places where customer/client data might be housed. And they must be able to detect, in real time, any 'cyber activity'—an attempted (or successful) hack, a virus infection, a phishing expedition where an unsuspecting staffer clicks on a link that leads to malware and, well, there are now a variety of creative possibilities that have been developed by people who would like to take your clients' retirement money and put them into their own anonymous accounts.

Layered onto that, making the whole situation more complicated, are the various regulatory requirements—which are considerably more stringent for advisory firms than they are for, say, grocery stores or law firms. (For obvious reasons.)

The new challenge to keeping track of cyber assets is that most firms today have advisors and ops staff working remotely, so what was once one server is now multiple laptops. What was once one location is now many. Where data was once stored on the computer in a back closet, now it's in 'the cloud,' spread across your CRM, portfolio management, financial planning, email, and any of 20 or 30 other possible software categories, scattered among various server farms.

Independent review

To do a cyber assessment and provide that independent evaluation, Edelman and his team will come into an advisory firm headquarters and do an independent review of all the various protections that the IT people have installed. At the most basic level, there should be individual protections installed on every device. If Edelman feels comfortable that this has been taken care of, he'll move on to the next thing to check. If not, he'll install the safeguards himself. "If an advisor is connecting a laptop to Redtail or MoneyGuidePro," Edelman says, "theoretically, it would be easy for somebody to steal that laptop and download the data on a whole book of business." The solution is a protection tool—Edelman prefers something called ProtectIT—which automatically handles a number of defensive functions.

"You log into Redtail," says Edelman, "and if ProtectIt is installed, it will immediately inventory the device, and say, *this Windows computer is encrypted, it has screen-saver locks and it has antivirus on it*." Collectively, it gives the advisory firm an automatic, real-time inventory of all the computers that are permitted to tap into its tech ecosystem.

In the rare instances where there is NOT an antivirus tool on all the computers, Edelman will add that as well.

The advisory firm's network will typically be protected by a firewall, which monitors entry and exit of messages and data. But Edelman says that not all IT firms know how to configure the settings appropriately. "We audit the settings and, if necessary, put them in good order," he says.

Edelman will also check the software settings, and some of them are easily overlooked. "When you buy Office 365, it doesn't come secure by default," he says. "You need somebody to do a security scan to make sure it's at the top level of security." There are a surprising number of administration portals, options and configurations, some of them residing in the Azure Active Directory, which enable the enforcement of multi-factor authentication for users and administrators, protect privilege access and institute automatic session timeouts/sign-outs. Do user passwords expire after a certain amount of time? Are there strength requirements for passwords? Does the system enable the automatic download of updated security patches?

Today's cybersecurity challenges have been magnified by staff people working remotely, and all client data stored across multiple programs in the cloud.

More broadly, Edelman's firm will install Data Loss Prevention technology on the advisory firm's system. "That would prevent an end user from, for example, downloading client data from Redtail and delivering it to Dropbox," Edelman explains. "Not only do you have to have controls to protect against external bad actors; you also have to protect against internal bad actors, and more importantly, you have to have tools to protect against internal, non-intentional bad actors."

For example? "You have an employee who goes to a website that tells him there's something wrong with his computer, and says to call this number," says Edelman. "They call the number and let somebody into the computer." That website might not be on any bad address list yet, so it won't be protected by ProofPoint, and now the bad actor IT firm has access to the computer. "He may install legitimate software like Dropbox," Edelman continues, "and then synchronize all the documents off of that device download them and then blackmail the firm."

Of course, Edelman makes sure that the operating system has multi-factor authentication, so that even if bad actors manage to get hold of your password, they can't access the tech stack. "With the right software," says Edelman, we can see that they tried to access the system, and more importantly, it would uncover where the bad actor was. The point," he adds, "is that you don't just install virus protection and feel like you're protected from bad websites, because the bad actors today are smarter than that. It takes program management, and a more advanced technical control, to keep a firm safe from these bad actors."

FCI's full cyber audit

Inside Information is published monthly

by Robert N. Veres.

Editorial offices:

Box 730
Tryon, NC 28782
E-Mail: bob@bobveres.com

might simply bless the protocols and softwares that are in place, it might involve turning on or off certain settings, or it might involve installing something that's missing. In all cases, it will involve ongoing monitoring of an advisory firm's tech interactions in real time—meeting the Cybersecurity Framework requirements (and SEC and FINRA regulations) that all 'incidents' are immediately detected.

If a breach occurs and client assets are lost, and the RIA doesn't have rigorous safety protocols, then it becomes suspect number one to the FBI.

Edelman will also recommend training systems if the advisory firm doesn't have them in place (KnowBe4 and ProofPoint are examples) that will help prevent the staff from making innocent clicks that open up security breaches.

And FCI also requires that advisory firms adopt certain protocols. "Whenever our protection goes on a device, we require the firm to have a decommissioning process, which is typically not done," says Edelman. "Meaning: if an advisor was using a laptop to access your technology remotely, and you want to get that device off your system, there is a process that we help you through. We want evidence that you either destroyed the device or properly repurposed it, so that whatever data was stored on there isn't at risk."

FCI is working with the professional liability insurance carriers to provide assurance that their policyholders have full cyber protection, which can lead to discounted pricing. "The insurance companies have noticed that the loss ratios of our clients is significantly less than their peers who are not working with us," says Edelman. That can involve protection and also mitigation. "If a company lets somebody into their system, and we or they pick up on it, we can take immediate action to keep the data safe," Edelman adds.

Edelman says that he has seen cases where a breach occurred, and the advisory firm discovered that the aftermath was a lot more complicated than just filing a claim and waiting for the insurance company to make the client whole again. "When money is involved, the FBI typically gets involved," he says. "And the first thing they do is ask whether or not you were negligent with your cyber program. They'll ask if you've assigned somebody to be in charge of cyber, and whether you have controls in place to protect your systems. If a bad actor hacked into your system and requested a wire transfer to Bulgaria, and your client acted on that, and you can't prove it wasn't you," Edelman adds, "then you're suspect number one."

Cost? FCI charges by the device; Edelman says that there's an up-front implementation fee, based on the size of an organization, for providing the initial inventory, fixing the settings, installing software—and the typical cost going forward is $50 a month per device for 24/7 monitoring and endpoint protection.

From regs to processes

But then, of course, you have to meet all those cyber-related regulatory requirements, right? That means installing procedures and keeping track that you actually followed through on them, so you can show this evidence to a skeptical SEC or state auditor.

Is there a convenient way to get a handle on those?

The key word here is 'convenient;' there are now so many pieces to the cyber regulatory structure that a sane person could not possibly keep track of them. To illustrate how complicated this has become, a firm called Buckler (*www.buckler.app*) has created a graphic, reproduced here (following page), that shows how a sample policies and procedures manual (right side) will map, policy/procedure by policy/procedure, with the mind-numbing array of (sometimes overlapping) regulatory requirements (left side).

Buckler is an app that creates template cyber manuals that advisory firms can customize and use in their operations. The app also makes it easy to transfer these various activities to a cyber compliance calendar that the firm can follow throughout the year.

The template cyber manual is 27 pages long, but it is broken down quite logically from (page

3) creating a cyber program and having it approved by the firm's board of directors or senior officer(s); naming a Chief Information Security Officer and outlining recurring tasks, to (page 5) purchasing cybersecurity insurance and providing evidence of compliance with its requirements, and tracking changes in the firm's tech stack in real time, to (page 9) having a way to document any significant business disruptions and having encrypted backup of all data, to (page 14) having security risk assessments of all tech vendors, all the way out to (page 27) insuring that remote access to the firm's networks and systems meet certain requirements, including multi-factor authentication and virtual private networks for any data in transit.

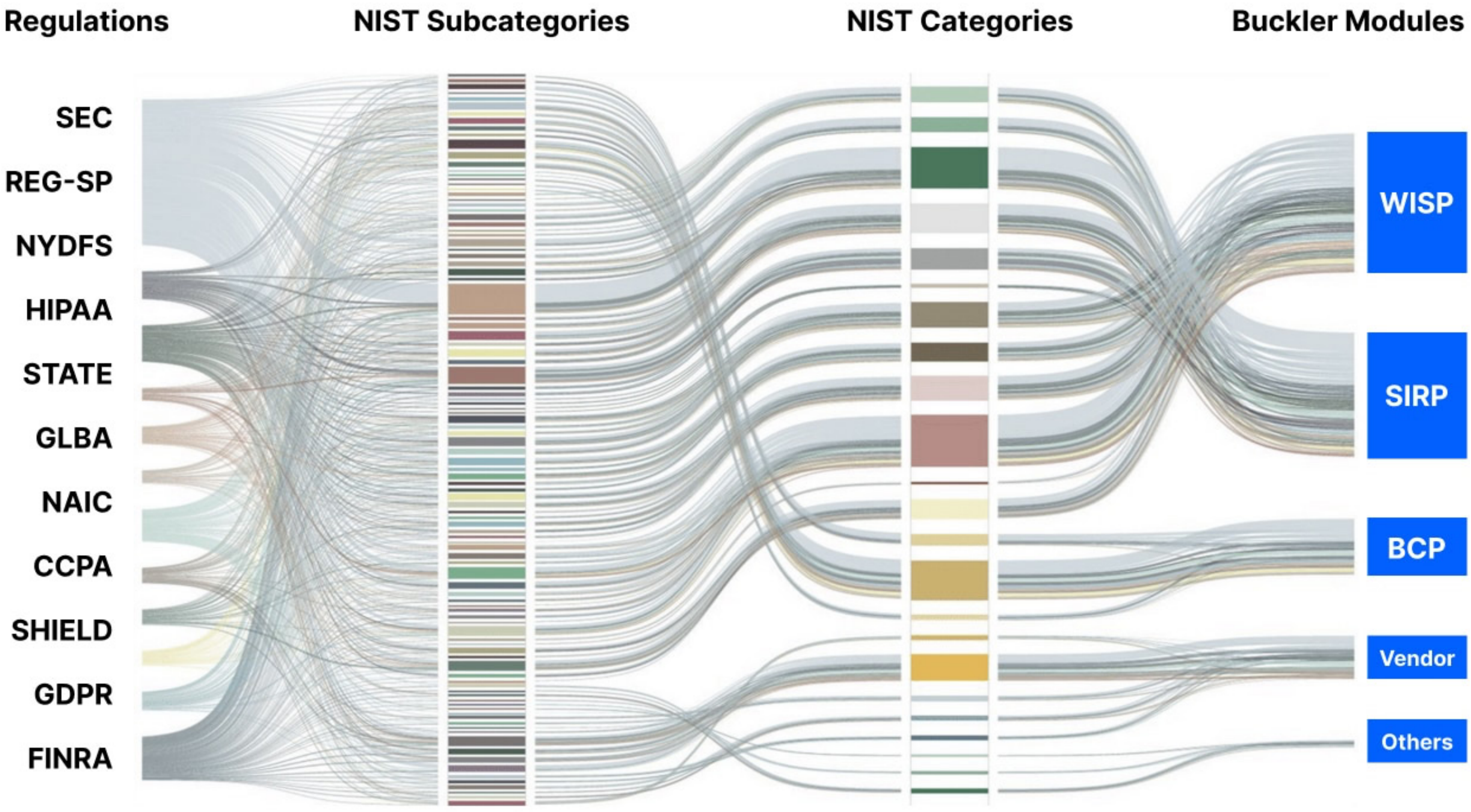
There's a lot in between, but most of it is common sense, spelled out in plain language, describing things that many firms are already doing.

"The policies list is quite long," admits Vincent Guyaux, who founded Buckler after working at FCI for six years. He says that the idea behind Buckler came when FCI had trouble finding a vendor that would complement the service package.

"We would install the technical controls, antivirus and firewalls and everything," he says, "and then we would ask if they had a cyber program and information security policies, and most of the time they did not. At first, we would say that we'd find a program for them. But after a lot of searching, we couldn't find anything that listed the policies and also provided a task management solution, with a calendar and a policy match—where, if you do that policy, how does it match up with the SEC or FINRA regulations?"

The cyber compliance system lived in Excel spreadsheets at first, provided to clients of FCI, but as it evolved, Guyaux decided to start a separate firm. "FCI applies the policies with technical tools," he explains. "Buckler is talking about the policies themselves. I spent hundreds of hours reading the regulations published or issued by the SEC, FINRA and New York Department of Financial Services," Guyaux adds. "We are matching all of those various policies with a simplified, streamlined list of policies here on Buckler—where maybe 30 regulations can be addressed with a single policy."

The policy template—which, to repeat, is designed to be



customized—also specifies who should be responsible for different activities. “The board of directors needs to set the overall cybersecurity policy,” says Guyaux. “They need to receive reports whenever there is an incident, and they need to name their CISO. The IT team has 20 or 30 policies that they are responsible for. The management team reviews and manages the access rights. You can assign each policy so that different people are owners of different policies, so it’s clear who is responsible for managing each of them.”

The value of the template cyber manual is that it maps every action back to the language of the regulation that requires it.

Once you have the template customized to your firm, you can log into the Buckler app. The active policies are all resident in the system, and Buckler offers links that will take the user to the regulatory language that gives rise to the need for each and every policy. “I click on the policy, and it calls up the actual SEC and FINRA regulation that it addresses, and you can see the exact language spelled out,” says Guyaux. “It’s helpful for whenever somebody asks, *do I really have to do this?* You have the proof right there.”

Guyaux adds that the SEC has actually published 15 documents related to cybersecurity over the past 20 years, and all of it is referenced and linked to Buckler’s policies manual.

The dashboard also contains a place for documenting incident reports (pages 10 and 11 of the policy manual), and a scheduler that lets the firm check off the various activities that the regulators require. “There are 37 steps generated in the system that have to be managed quarterly or annually,” says Guyaux. “You put them on a schedule that you create, and you can check them off as completed, so you can demonstrate completion to the auditors.”

An example is a phishing simulation, where phishing emails must be sent to the staff members to check their awareness of potential threats, and help them know what not to click on. This might be handled quarterly, and if it wasn’t completed, the system will generate reminders. Another task is changing passwords for the public wifi system. Another is annual review of the business continuity plan. Another will be an assessment that the logs of the network and computers are working. Another is testing the data backup system.

In each case, Buckler will send reminders of the upcoming task, and mark as overdue task that hasn’t been checked off. Your chief information security officer can see the list of upcoming and completed tasks and the scheduled or completion dates by scrolling down.

The point here is to break down what is really a very complex regulatory requirement into manageable pieces, track the completion of the things that the regulators require, and be able to show the SEC auditor (or, heaven forbid, the FBI), with the click of a button, that these tasks have been completed in a timely fashion.

Vendor assessment clearinghouse

Remember how, on page 14 of Buckler’s cyber policy manual, it mentioned having security risk assessments of all tech vendors? Chances are, you paused a moment at that item, because, well, who can actually get the various companies in your tech stack to provide you with the required security attestation? Who even knows what that entails?

“The regulators are telling advisors to make sure their vendors are secure, that the data they have on your clients is secure,” says Guyaux. “You should do an annual assessment that you can put in the files, so the regulators can see that the vendors are secure. But in many cases, you contact the vendor with your request, and you don’t get any response, so that file is empty. So you put in your checklist that you tried to get that data, and that’s what you show to the auditor.”

On the other end of this requirement, Guyaux says, the vendors are put in a very difficult position. They need to find a way to respond to many thousands of requests for audit data, and of course everybody will be asking for this data in different formats.

Buckler is in the process of creating a solution. "We've sent a 50-question security questionnaire to 479 different vendors in the financial services industry," says Guyaux, "and as we collect their responses, we'll create a clearinghouse where advisory firms can go in, for free, and pull out the comprehensive, detailed attestations of their software vendors for their files." Participation in the clearinghouse will also be free to the vendors.

The 50 questions ask, for example, if the firm does or does not have risk assessment policies to identify, manage and mitigate cyber risks relevant to its business. Every vendor should, as a matter of routine, be able to provide a 'yes' answer, but the potential answers include 'yes with evidence,' and asks for that report. If the answer is 'yes without evidence,' then the vendor would indicate in the 'details' field why it does not have evidence and its plan to obtain it.

Question 7 asks the name of the firm's CISO; question 9 asks whether the firm maintains cyber insurance that covers losses and expenses attributed to cyber breaches (and asks for details of that policy), question 18 asks if the firm has a complex security password policy for endpoints, software and systems; and question 33 asks if the firm performs background checks on its employees, contractors and affiliates who access, control or store private data.

Guyaux says that these are all things that these firms have to do as a matter of business routine. Putting the attestations and evidence into a single compliance file for any advisory firm to download for its own folder should theoretically be a huge time-saver. The collection of vendor data is ongoing, but Buckler should have many of the most popular programs in the clearinghouse by early next year.

Buckler is creating a clearinghouse of cyber due diligence reports on the fintech vendors that advisors are required to have in their files.

Cyber training and assessment

Is that all? Almost. There's a new initiative that could impact this discussion in the very near future, jointly created by Tod Arbutina of Three Cord True Wealth Tax Solutions in Beaver, PA and Guyaux at Buckler. Arbutina became concerned about the security of his data when he discovered that a prominent broker-dealer was selling meta-data and also had experienced two data breaches in the same year. More generally, he is concerned that his client data is stored in multiple locations in multiple programs, and that some of the custodians seem not to be totally sure whether that data belongs to the client, the advisory firm, the custodian or all three.

"I don't think most clients realize how dispersed their financial data is when they work with an advisor," Arbutina says. "When the advisor onboards clients, they should clearly disclose what their digital ecosystem looks like, and what kind of security, privacy and control is in place. Most advisors don't do anything like that currently."

This led Arbutina and Guyaux to develop two separate but related initiatives. The first is a program that would allow advisory firms to obtain a Digital Asset Fiduciary certification—which would distinguish them in the marketplace as vigilant about protecting client data—and, further down the road, an audited Digital Asset Initiative (DAI) report, with what amounts to a data protection score.

The certification process currently includes an overview course entitled *21st Century Fiduciary and Digital Asset Fiduciary*, which outlines various different cyber responsibilities. The coursework is accessible in the form of videos here: *https://digitalassetinitiative.com/*, and completion entitles the advisor to a Certificate of Completion awareness badge.

Sometime between now and the end of next year, the program will feature an assessment of an advisory firm's digital ecosystem, leading to a DAI score, whose components will include working with an outsource cyber service provider and various attestations, with a cyber audit process that is under development. Arbutina's firm is a test case for this report, working with a currently undisclosed vendor and a cyber department at one of the universities, who are evaluating potential best practices. Each firm score would be coded red, yellow or green, green being the most secure, red being something that might cause Edelman to faint from alarm when he checks over the work by the local IT person.

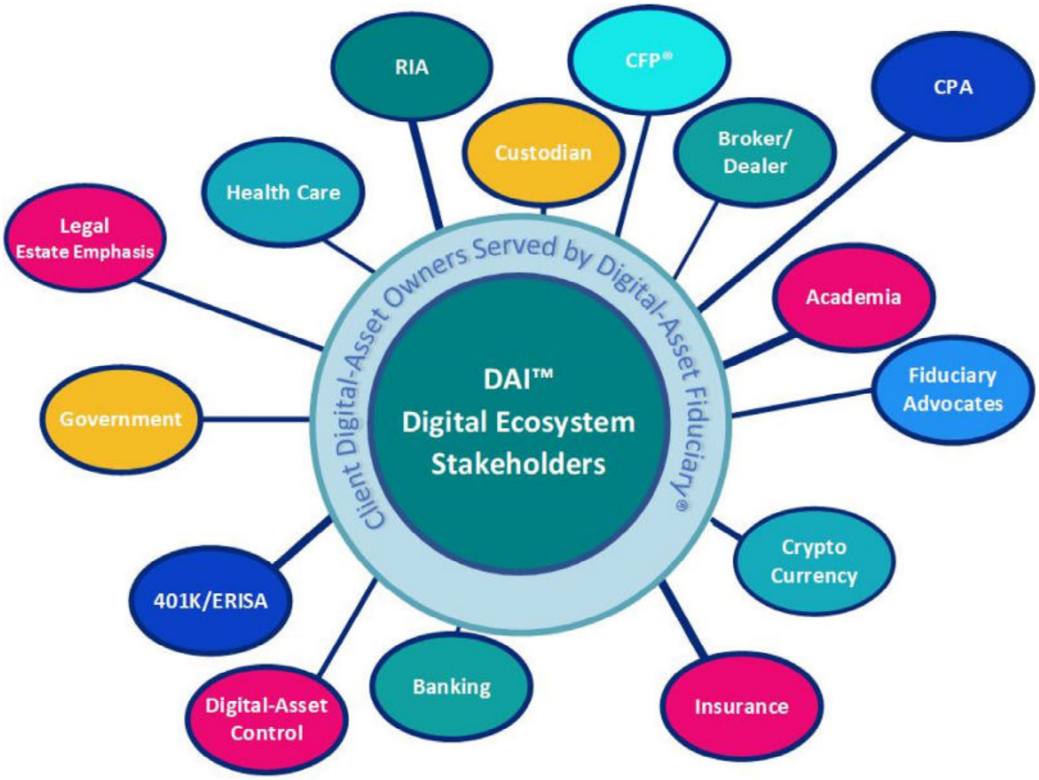
Further down the road is something that Arbutina describes in more idealistic terms; he's working with several vendors who would create a single data hub that all the various components of an advisory firm's tech stack would access—and the client data would live in the hub, not in the various programs in the cloud. The data would be portable; that is, the clients would own that data and be able to take it with them should they change firms or should the advisory firm change software vendors. (If you're not clear on what that would look like in a software ecosystem, look at the explanatory image below.)

"The fact that today all of that data is sticky, and that clients have to give out their information all over again when they're moving from one advisory firm to another, is fiduciarially inconsistent," Arbutina argues. "If the client wants to fire us, they should be able to take their information and move on." He's identified a vendor that will create that portal, but the initiative is still in the early stages.

Our annual software survey (which is live: *https://www.surveymonkey.com/r/HB3GSP8*) tells us that few advisors (15-20 percent) are working with a cybersecurity vendor that specializes in our profession, and many advisors seem to regard the procedural rigors of protecting client data more as an inconvenience than as a necessary component of client service. But this article suggests that the inconvenience factor can be tamed, and that the separation of duties (IT installation and cyber overview) can strengthen the protections and maybe even qualify advisors for a discount on their liability coverage.

All it will take is a high-profile breach, and some FBI attention, to make this topic more relevant to the profession. The available tools and services are growing more sophisticated, and there are initiatives that will make it easier to acquire the awareness and install the procedures which would make advisory firms a much less tempting target for digital attacks.

Meanwhile, I invite you to take our survey. And if you run into Joel, please tell him that you're much more committed to effective cybersecurity than you were before you read this article. It might help him sleep better at night. ■



Copyright © 2022, Digital-Asset Intitative™. All Rights Reserved.