Cloud Technology Roundtable

Five financial services executives presented their views in a roundtable discussion moderated by Marie Swift and held in conjunction with Schwab IMPACT 2014.

Sponsored by

RIGHTSIZE SOLUTIONS
Strategy. Security. Service.

Context / Setting

Following the Schwab Impact Conference in Denver in November 2014, Marie Swift of Impact Communications sat down with five attendees for a roundtable discussion on cloud technology. The 60-minute conversation was a spirited debate. This paper presents just a few of their important insights and observations.

Participants

- Zohar Swaine, Mink Hollow Advisors
- Wes Stillman, RightSize Solutions
- Roger Kruse, CFP®, ChFC®, EA, FFP Wealth Management
- Scott Kahan, CFP®, Financial Asset Management
- Matthew Dorchak, Keene & Associates

Publication Notes

Individual video clips and a digital version of this white paper transcript are available at AdvisorsThinkTank.com. Videos and roundtable production services were provided by Impact Communications, Inc.

Inquiries about this Paper

Leesy Palmer, Director of Media Relations, Impact Communications, Inc.

(800) 974-7753 | ImpactMediaManager@ImpactCommunications.org

Cloud Technology Roundtable

MARIE SWIFT, President, Impact Communications: The rise of cybersecurity attacks, especially involving financial institutions, is cause for growing concern among today's advisors for themselves, as well as their clients.

Today's investors are more tech-savvy than ever. It is not just the future clients from the millennial generation. Older clients are defying stereotypes by showing up with iPhones and iPads, as well. The Internet age has made today's investor very different than even five years ago creating a 24/7 demand for information to be received when, where and how they want it.

Today's discussion will address the following questions:

- How can advisors adjust to the risks and concerns over cybersecurity while still accessing the benefits of cloud technology?
- What role will technology play in the evolving demands and needs of current and future clients?
- What are the biggest technology challenges and opportunities facing financial advisors today and in the next one to three years?

Roger, will you go first? What are your key compliance and security concerns?

Compliance and Security Concerns

ROGER KRUSE, Founding Partner, FFP Wealth Management: I'll say that it's not so much what I think I'm missing, rather it's what I don't know. What I don't know pertains to all of these big breaches on the banks. How susceptible am I to some Russian hackers slipping in? I don't really know the answer to that. I feel like I'm safe, but because it's been in the media a lot, security has been on my mind. If I'm swiping credit cards – which I do in my office – is that causing me to open something up that I didn't know I needed to worry about? It's just little things that came out of these recent data breaches that caused me to step back and ask, "What don't I have? Is there anything that I don't know about that I should have?"

SCOTT KAHAN, President, Financial Asset Management Corporation: I would agree. It's what we don't know that is the biggest concern, especially for a small advisory firm. You

know a lot of people think small firms fly under the radar – the hackers aren't looking for the small firm. But I find that a little naive and probably not accurate. My feeling is that anybody is susceptible. I can't even figure out the trails of how a credit card gets through and it's a little bit scary. It's not a matter of if but when. Are we doing the right things to implement every precaution?

MATTHEW DORCHAK, Portfolio Manager/Analyst, Keene & Associates: What concerns me is, if a client leaves their email open while at a local library that includes some correspondence from me, and the hacker is able to gain access to their e-mail. Then the hacker starts asking for a wire of funds. I am more concerned that the hackers are getting braver and a little more aggressive in their attempts to obtain my clients' assets. We try to continuously stay aware of these situations by listening to our custodians take on compliance, and not maintaining custody of clients' assets. However, this continues to be an increased risk.

KRUSE: I've had a similar experience and am very concerned about making our clients realize just how susceptible they are. I had a client who received a call from someone saying, "This is Joel with your virus software company. I see that it's not working. Will you let me in to fix it?" The client literally let this caller into their computer and the next thing we knew we got a phone call from Fidelity saying their account was being liquidated. So clients are susceptible and we need a way to raise their awareness or concern about talking to people on the phone, opening their computers to people who are calling to help fix their computers. That is happening.

WES STILLMAN, Founder, RightSize Solutions: At RightSize we try to alert our advisors about scams and other security risks – you have been seeing those alerts on a variety of issues – you could be sharing much of that information with your clients. We strongly believe the weakest point is the end point, the end user's devices. This applies to advisors as well. Mobile devices, for example: do you carry personal email on the same device you use for your work email? Your answer is probably yes. So, those things can be a point of vulnerability. Even though it has nothing to do with work, if the device is infected there is a very high probability that your corporate email will also be compromised.

KAHAN: Being in a small office we feel we implement as much protection as possible with our employee's because we look at their computers. We check what they are doing personally to ensure there are no real issues – they have security protection and passwords on phones and mobile devices if they are getting their office email there. We've had cases where we got an email from a client, telling us they were stuck overseas and needed money wired. You suddenly realize this is not a normal conversation from a client. I've heard stories about people that follow through with these requests, but you really have to know your client well so that you know what kind of communication you normally have with them. Back to the point of protecting different devices, when a client isn't home they are going to their computer, maybe their kids are using that same computer and you don't know what kind of doors they've opened.

SWIFT: Where do your responsibilities start and stop?

KAHAN: We look at it as our responsibility to make sure that everything we do for the client is protected just like we were managing their money. Making sure their retirement, education, everything is taken care of. Making sure there is protection of anything we are sending them. There is only so far we can go, though.

We should be able to provide them with more information. But will they follow through with it? Will they put the right protection on their computer and devices? We can't control that. It's better for them, better for us and everyone involved if they do follow recommendations.

STILLMAN: I think the most responsible action you can take is to utilize everything within your power to protect information within your control. Obviously you cannot control what goes on in a client's house. But it does not stop there. We have heard from several clients that they are concerned that a client may come back on them even though the breached occurred on the client's own computer and/or due to the client's lack of security. We advise that you, the advisor, must be able to prove that you are doing the best job that you can to protect your client's information while it is in your control. Any experience with auditors on this subject?

KRUSE: We will know next week (everyone laughs). I'm having an audit being done in my office right now. We must have everything turned in. Interestingly, the one thing that wasn't on the list was our security policy. But I know they are going to ask for it when they walk in the door, so we will be prepared for that because a security policy is the hot ticket today. Everybody is concerned about it. For the regulators not to put that on their check off list tells me it's just one of those things they will surprise us with. I've had plenty of audits in my life and I'm not afraid of an audit. But I believe that security is such a high interest area that I

> *"I am very concerned about making our clients realize just how susceptible they are."*
>
> *~ Roger Kruse, ChFC®, CFP®, EA*

want to be more prepared for it than ever because of recent issues that bring it to the forefront.

STILLMAN: So here's the good news for you, Roger. Since you are a RightSize Solutions customer, we offer you all the right protections: two factor authentication, network security, antivirus protection, etc. But really it still comes down to your security policies and how you want those policies implemented. Everything we do is a customized solution. Your policies may be different than Scott's or Matt's so, from an infrastructure standpoint we have all the capabilities to implement your individual policies. What's interesting to me is the due diligence that auditors are going to ask you about. What did you do? How did you do this? How can you prove to me that you are doing it? It is one thing to have policies written down and quite another to produce a report that demonstrates you actually do what your policy promises you will do.

> *"It is one thing to have policies written down and quite another to produce a report that demonstrates you actually do what your policy promises you will do."*
>
> *~ Wes Stillman*

SWIFT: So from your perspective, when you look at what is being done to protect your firm, what questions or thoughts enter your mind when you think about security?

Setting and Enforcing the Policy

KRUSE: I came from an in-house network server in 2010 and knew I wanted to move to a new environment. It seems like computing took up an enormous amount of my thought process in a day. Transferring all of the backup and the technology and the updates off of my table at first make me more productive in the office and allowed me to focus on something other than technology. Now I feel, maybe I don't think about it enough. But I feel at complete peace that things are getting done. I don't have a server in my office. When somebody does save something on a desktop, I don't do a write up but I tell them you save nothing in these computers. Is there a way we can make sure they don't save to their own computer?

STILLMAN: That's a great question. Yes, RightSize Solutions can enforce that policy. We can prevent things from flowing between a local PC or tablet and your private remote environment. In fact we have several clients that have that policy in place today.

KRUSE: But what if they scan something and work at it on their own computer and just leave it as that? I don't know if we can do anything about that.

STILLMAN: The reality is that the answer is no. You can't control everything that your employees do. If you don't give them some authority and some keys to the kingdom they can't

perform their jobs. There has to be some amount of trust in the employer / employee relationship. Since smaller firms tend to have fairly highly skilled employees that perform a variety of duties, it is not realistic to think that you can prevent an internal breach. That said, I believe you can put realistic controls and monitoring tools and processes in place that minimize the risk.

ZOHAR SWAINE, President, Mink Hollow Advisors: From a regulatory scrutiny perspective, it's about creating the controlled environment that enables and enforces a set of rules and standards. "Rogue traders" may always find a way around imperfect environments. Consider a huge institution such as Bank of America (BOA), who was recently "hacked", despite their best efforts to prevent. Millions of dollars spent in prevention and it still occurred! The key is to be sure we have the policies and procedures in place, with appropriate monitoring of rules appropriate to the environment and risk levels.

> *"The 24/7 demand from today's clients comes at the expense of technology's security."*
>
> *~ Zohar Swaine*

A Matter of Trust

DORCHAK: We live in a world where trust is sometimes overlooked and something that needs to be revisited. I agree there is no way to stop someone who is persistent on doing harm; however, coming from a small firm we have a different set of risks when it comes to who sees our data. For example, we use a technology company that processes our custodian's data every morning; that's one of my risks in the cyber world. I'm hopeful that I've done my due diligence and gone to great lengths to interview companies for services that I need. We took direction from our custodian, and then did in-depth research on the company.

SWAINE: You bring up a key point – trust. We are an industry that quite literally has built its foundation on trust and to your earlier point, Wes, when dealing with the BOAs of the world, they have created these seemingly iron clad infrastructures. In our environment, it's a very different ecosystem of providers and hires and whatnot. It is incumbent upon us to do what we can. Wes, you started to bring up mobile devices. Whether you are enabling employees to use their own smart phones, perhaps not as well protected, or other devices…that is where the thin ice resides. I'm curious to know what each of your approaches is or if your colleagues have restricted mobile devices in any way?

KRUSE: So at FFP Wealth Management for many years we just did not allow those connections. But as technology improved and I developed the desire to have a smart phone myself, we opened the door to allow staff to use their devices – but it made me very nervous. There is something out there which I learned about from RightSize that has the capacity to flip a switch and delete everything. I'm not exactly sure what everything means but whatever gets lost, that's a concern. I've walked away from my phone and gone back and it's still there but knowing whatever is on there can be disintegrated electronically gives me some peace of mind. I opened it up to my staff. Two or three in the group started to use their cell phones for emails and to connect. Several have laptops will which they will connect. I've provided most of them with laptops but I think they are used for more than work. We can tell them to never use the laptop for personal use, but I'm sure they do. The ability for people to work remotely is why we are doing this. We have to know we are at the beginning stages of determining how manipulating this new world of data and technology is in a way that allows us to be productive but not sloppy. We have a policy of changing passwords and password protections. We have policies where we use our work email for work only – not personal use. We draw a really tight line on that. I don't' know if we monitor that but my goal for the entire staff, including me, is to never have a personal email in our work inbox. I save them for infinity and then can be audited. The regulators allow emails to be deleted, but if you delete emails you must be able to prove that a client's email did not get deleted. We cannot do that. So our policy is that we never delete emails. We've developed this policy so that our employees will consciously separate work and personal email. We know that once in a while something comes in that shouldn't. So the goal is to have that message transferred to their personal email. We don't want that in the work email.

KAHAN: Regarding personal email, in our office we let employees know that I have access to the personal email once it's transpired through the business email system. We discuss this separately from security issues. I don't think they want me to see their personal communication and I don't want to see it either, so that pretty much takes care of that issue.

Regarding clients being able to contact people or an advisor; even if you don't want to get your email today remotely, you really have to because clients expect responses quickly. But it's a matter of quality of life. Sometimes employees have things to do personally, and we want people to be happy at the firm. So if they need to go separate from a doctor's appointment or

they need a day off or they want to do a family event, it doesn't make sense to say "Ok, that is fine but then who is going to check your email?" The clients expect responses pretty quickly. Employees know that if they are out on a personal matter and they have their phones, then they can respond to email if they feel the need to respond. The clients are expecting that.

SWAINE: You are right. I think the 24/7 demand from today's clients comes at the expense of technology's security.

KAHAN: Another point regarding 24/7 attention is that there are times when I don't want to answer emails, but I've trained my clients to expect a response even if it's 11 o'clock at night or a Saturday or Sunday. We had a situation within the last year in which I didn't respond right away. The client called the office asking if everything was OK with me. Also, if I don't respond all weekend, then I come in Monday morning and have a stream of emails to deal with. If I can deal with them as they occur on Friday night, Saturday or Sunday, I get them off my to-do list. Then I can come into work Monday morning without losing half a day replying to email. It's a timing issue, too.

STILLMAN: I want to go back to a point made earlier – RightSize clients have security coverage because we can wipe a phone. But what if the device is lost? More importantly we recommend that you implement a policy regarding the use of passwords and encryption on all mobile devices as well as the use of two-factor authentication. We believe it is a real liability to your firm. I think it is a fairly common practice to allow your employees to access company email and systems via their private devices. People like their phones and it's convenient not to carry multiple phones, so the point being if they have access to company information they absolutely must adhere to your rules and policies. I think it is important to consider the extra concerns personal devises pose when a phone is lost or someone in the company says they need to wipe it. We encourage our clients to spell out these policies in your employee handbooks. It's important that staff understand that if they use their personal phone for whatever company purpose it may be wiped. And it's just not a corporate email that is going to be wiped; it's going to be the whole phone. It's a necessary evil.

Best Technology Practices

SWIFT: Let's talk about some more "best practices."

STILLMAN: Matthew brought up a very good point. Today he uses an offshore service. That's a special exception and only for Matthew's environment. RightSize actually blocks most out of country access. Any provider out there is going to provide anti-malware protection, scanning, intrusion detection, etc. We believe it's important that every single one of your devices be protected. If you are accessing your remote private environment or even a business web site like Schwab from your mobile devices, then we recommend you consider two-factor authentication.

KAHAN: It goes back to the point of sending an email to a client from your protected phone. They open it up on their phone and respond, unknowingly opening up a door you don't want to have opened. It's difficult to enforce something like that. We can only make clients knowledgeable. Provide them with resources and information and if they are like most people, they'll think, "Oh, that's nice I'll get to that when I get to it."

SWIFT: How do you think your clients would respond if you provided a secure email account for them to use?

KAHAN: Actually, I think clients would appreciate it. But it depends upon the client whether they will use it or not. It means they have a different email than the normal email and that means another email account. That's where I think it breaks down.

DORCHAK: One of the differentiating factors we're considering is a portal through our home website with a unique identifier. We would use the technology for some of the following: their personal quarterly reports, a story we think is worth reading, or a congratulatory message about a life accomplishment. An office "everywhere" is how the world is working. No more brick and mortar. I think that's why we are seeing depletion of office rental space for the previous 10. The virtual space is vastly growing. For example, if people call the office, it's pushed directly to our cell phone. Everything is on our cloud based servers. You want some documents? Great, request them. I will get them for you no matter where we are. It actually would make me feel a little safer having everything in the cloud. I believe it is part of our disaster recovery plan.

"It actually would make me feel a little safer having everything in the cloud. I believe it is part of our disaster recovery plan."

~ Matthew Dorchak

Safety in the Cloud

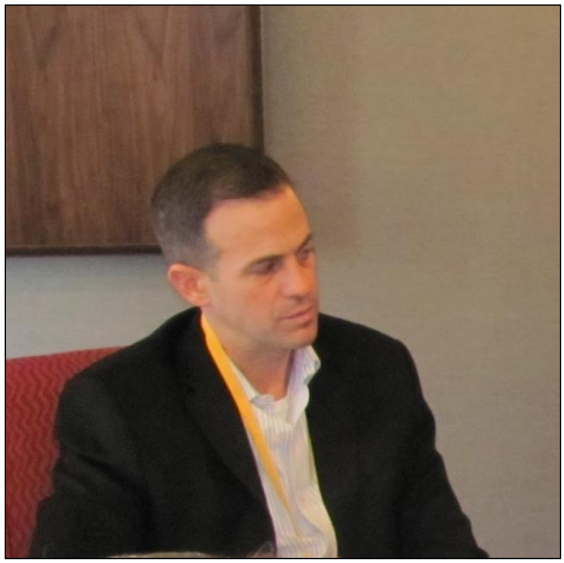
STILLMAN: Ideally, cloud safety entails some kind of secure wrapper or environment which can be accessed through a secure connection or portal to the rest of the world. It's the end devices that are difficult to manage. Whether a PC or a laptop they are carrying around or a phone, they are difficult to manage. The trick is getting security on every device and then managing them to ensure the security is up to date. The fact is; one will spend an inordinate amount of time managing all of the devices. Consider this scenario: You access your business applications via a device connected through a 4G connection somewhere or even your home router. Maybe you have teenagers at home that don't care what gets loaded to a particular device. If you use that computer and it's infected, then you probably have some kind of breach on your hands.

We see a lot of people going to cloud based applications. Why? It makes things easier. You had a CRM on your desktop then found a cloud based CRM that you like better, so you switched. The interface is updated and it is accessible from all of your devices. Setting aside the issues around individual devices, here are two key questions to ask: Do all of my cloud providers have all the security I expect them to have? How do I learn what those security features are?

SWIFT: What are some of the myths out there that are just wrong regarding clouds based security? Where are people wrongly placing their trust?

STILLMAN: First, I think there are a lot of misconceptions regarding what the "cloud" is! It is not some magical, mystical thing out there somewhere. The servers are real hardware managed by real people, housing real applications that were written by human beings.

Secondly I think there are a lot of myths about hacking. For example, hackers grab things out of the air or from the Internet on the fly. That's just not how most of the hacks occur. Hackers are like any other thief. They are lazy and typically take the path of least resistance to access information. It is plausible that someone could grab data off your Wi-Fi or network and maybe reassemble the packets and decrypt the data. However, it is a lot more likely that a breach of data will be accomplished by gaining access to your systems through you, the individual.



SWAINE: So the other half to that question is, where do people believe they are airtight in their security but in fact it is a false sense of security?

STILLMAN: People believe that a cloud based application must be secure because it is in the Cloud. The fact of the matter is that every application, whether it is web based, cloud based or windows based, executes on some sort of server storing data on a physical media somewhere. Further, there is at least one or more IT administrator that has access to that data. When moving to the cloud, you have to do your due diligence on your provider? Is your provider storing your data with another provider? Do you know where your data is located? Do you understand who has access to this data? A lot of people in the industry are blindly accepting that putting their cloud based application with Amazon and Rack Space is a very good thing.

SWAINE: This is an interesting environment we find ourselves in. On the one hand we have the cloud, which is a relativity new concept to folks and delivers a false sense of security. On the other hand we have auditors that frankly are not asking the right questions. Many of our colleagues and advisors that are much smaller are not thinking about security in the right way. How do we take the industry to the next level of awareness with education? Is it going to take a watershed moment or something bad to happen before we start paying closer attention?

KAHAN: As far as a watershed moment what about JP Morgan, Bank of America? I have clients that say they don't conduct banking online because they don't want anyone to steal information. I say that is OK but keep in mind your data is already there anyway. If you chose to set up a login, your data is there. I think that is something that people simply don't realize. I want to say it's mostly older clients, but you also have older clients that are very savvy online. As a smaller firm we are using different providers than we do for due diligence and our homework but I don't know all the questions to ask because I learn as I go and I speak to a lot of different people. We assume that if they are well respected in the profession, and our peers are using them and we've done our due diligence as best we can, then it should be OK. It is

usually great until there is a problem. And when there is a problem we wonder where did it go wrong? By the time we learn to ask the right questions, it will already be outdated.

DORCHAK: I would argue some watershed-moments that have already occurred haven't been properly communicated to the masses. From a segmentation standpoint, everyone is segmented so if something happens at your firm, I would not hear about it in Fort Worth because it doesn't make national news. For example, if someone told me they were in California, in a $6 billion RIA and were hacked, I wouldn't know the name of that firm. Hopefully, there is an educational development going on in this business that somewhere that lapses over into the general populous about what exactly we do. I would hope that will be a benefit to the RIA community because we seem to be taking the high road.

KRUSE: When it comes to outsourcing and the different products and tools we use, I have downloaded and read the privacy agreements. Some of these services I've chosen not to use because one web meeting software said they can gather any information and use it anyway we want without restriction. I use another one now that has very tight security but I tried to imagine being deposed. It would go something like this: "Did you know what that said?" "Well, I didn't read it." "Well that doesn't work." "I read it and ignored it or I read it and didn't understand it." I don't have a way out.

Some software asks you to check the "I agree" box. That's a disservice to all of us end users that they would throw these items in these agreements because we become liable when they do something with our data. Or it gets lost from their end. I'm not sure I know how to resolve that and not sure I want to keep reading because pretty soon I won't be having any services. Of course they update these every so often and you log in and you can't use it until you click the "I Agree" box. What did I just agree to? What are we agreeing to when we sign up for service and how do we defend ourselves from the constant changes to what those agreements say. We pay the fee, they changed the agreement. We are trying to work. What are we going to say? No?

SWAINE: The terms and agreements you bring up is a very interesting point. As advisors you all know that we've gone through this period of writing financial literature in plain English and hopefully only in our personal lives guilty of scrolling to the bottom and clicking the "I agree" button. It seems to me that the industry, our industry, which is so dependent on trust and good security needs to come up with a common way of grading what is appropriate and what is not. There is no real way, it's very subjective. I would be curious to hear anyone's perspective.

STILLMAN: We believe that you have to include technology in the discussion. The SEC disseminates the guidelines and risk alerts – including the one on April 15th, 2014 that scared everybody to death. In our opinion they should have explained that the security landscape is changing and provided a better explanation as to the things that should be reviewed. We do believe that all regulatory agencies must continuously look at the ever-changing threats so they can help the advisors with best practices, due diligence and what they are going to be auditing. Unfortunately, when it comes to technology, the audits are more like preparing for a test only to find out the test is on a completely different subject. Of the audits we have seen they are beginning to include what technology should be in place, and best practices for managing the technology and the due diligence that should be done to engage technology providers. We think that these are good steps but need more clarification of what is acceptable and why certain technologies pose specific risks.

DORCHAK: I agree completely. And in my opinion, that's an added benefit of RightSize Solutions. One of the great things is having them to call whenever we're facing a technology issue. "Should we go with this or with that?" I always call RightSize and ask what they think about new technology. It brings me comfort and helps me sleep at night relying on great service providers. That's an added benefit I suggest you consider when screening who you will outsource to.

"There are firms out there that really take that pressure off, but it's still our responsibility as a business owner for our clients that we are picking the right providers. Everybody has to do their due diligence and do it properly."

~ Scott Kahan, CFP®

KAHAN: We got involved with outsourcing to RightSize after Hurricane Sandy. Losing power for a minute or two can be a big deal. During and after Sandy we lost power for 10 days. To be out of power in downtown Manhattan for 10 days was scary. The only good thing is that our clients were probably without power as well, being located in the same general area as our office. People that weren't in the area who had power knew they couldn't reach us and we did our best by phone. I said this is crazy. We looked for other solutions. Programs we use such as Portfolio Center, Junxure and MoneyGuidePro all have web-based solutions versus a desktop. So we started looking at that, too.

All these different programs and that's when I started to look at companies like RightSize Solutions to see which one would be the best fit and what came along with it was all the security. All the things I thought of but didn't really delve into. Then the IT part was just another added benefit. There are firms out there that really take that pressure off, but it's still

our responsibility as a business owner for our clients that we are picking the right providers. Everybody has to do their due diligence and do it properly. There are a lot of companies out there that are here today and gone tomorrow. The benefit really is security.

From our standpoint that is not what started it but we realized in making the decision that one of our biggest concerns was security.

DORCHAK: I'm reminded of the old adage, "out of chaos comes opportunity." The hurricane was the last straw for you guys.

KAHAN: Yeah and the interesting part is that where I live in West Chester County, we were one of the few homes that kept power. But I couldn't even log into servers or go into our office to carry the server down 10 flights of steps and to my home because we couldn't get into the building. It's not fun being out of business all of a sudden but you know, 10 days is out of your control.

Tip of the Spear

SWAINE: Just by virtue of sitting around this table, this group is at the tip of the spear. You've given thought and invested dollars and so forth. What do you tell your colleagues, or what do your colleagues tell you, who aren't around this table, telling you about technology security and where do you think their false securities lie?

SWIFT: Perfect, Zohar. I was just about to ask for closing statements, so would the three advisors at the table please do that now.

KAHAN: Similar to the false securities we have had at times, if we are using Schwab or Fidelity then a big firm must be covered and know what they are doing. But I also find that my peers, who tend to be smaller business owners, know the issues they have is staying on top of everything. Staying on top of servers and knowing the hardware. There is a hardware side and what drives your business and there is the security side which can really hurt your business. They are both issues and people coming at it from one or the other and not really realizing the benefits of the other side of it until they go into it and investigate it.

Outsource, outsource, outsource. It comes with a price. It's a financial price and a security price. I think it makes us more efficient in our office when we can take things off of the table. But we have to make sure the table we are putting them on is set properly and is protected, otherwise it's going to come back and hurt us much more than we could have ever imagined.

DORCHAK: Make sure that when you are evaluating service providers you do a little more than selecting a firm just because someone you know uses them. I also think there should be a level of detail that is covered by asking harder questions. There is nothing wrong with asking or saying "I don't know I'll have to get back to you." That was one of the great things RightSize was able to do for us. It was a three-month process back and forth with lots of questions. I think the cloud is a better way to go for the growth of the business, and for the growth of where I want to take the business in the next five years.

KRUSE: I have a couple of things to say. When I went from brokerage fees to fee-only services I did introductory seminars for all my clients. I had a CD playing and the last song that played before I got up to speak was Bob Dillon, *The Times Are a Changing*. We all have a tendency to want to hang onto that which has always been the most comfortable. Change is hard. When I look at my client base whose average age is 64.9 years old, people told me those people would never get a smartphone. But those people not only have a smartphone, they have an iPod or iPad because that is the only way they can stay connected with their children and grandchildren. If we are not moving our business to keep up with technology changes, we are going to be left behind. My clients are going to show me their iPhone with remote access and wonder why I don't have remote access.

Once you make the decision to change, then you have to do the due diligence and find the people that are solving the problems. What I like about RightSize is their focus on financial firms. They know our software. I don't call Junxure when I have an issue, I call RightSize. I don't call Portfolio Center, I call RightSize. We do as much as we can through RightSize. They can't solve everything but if we start there it gives me, as a business owner, a great deal of comfort that I have one principal point of contact for everything in my computer and if they can't take care of it they will redirect me to where I need to go. I don't have to figure out who to call. To me there is such peace of mind in that. That in itself makes it worth investigating into this company; otherwise, if you have 10 different apps, you have to call 10 different people and you might get a different person every time you call and you are never sure if you are getting the right answer. I'm always confident when I get an answer back including, "I don't know," which is an answer (laughs). If they don't know what to do, then they will at least help me find the right person who does know. That type of benefit is what frees me up to focus on developing my business and spending time with clients not developing technology platforms. I don't ever want to do that.

Roundtable Participants

Matthew Dorchak
Portfolio Manager/Analyst
Keene & Associates Investment Counsel
KeeneAssociates.com

Matthew Dorchak joined Keene & Associates Investment Counsel in 2012 where he performs analytical research involved and is involved in the selection of securities for client portfolios. He assists in the management of the firm's mutual fund portfolios, including the setup and maintenance of client accounts, monitoring of client transactions and activity, and execution of report preparation, daily portfolio accounting, and trading. Prior to joining the firm, Dorchak worked for an investment advisory firm and has extensive experience as an auditor. He holds a BBA in Accounting from Texas Tech University.

Scott M. Kahan, CFP®
President and Senior Financial Planner
Financial Asset Management, Corp.
FAMcorporation.com

Scott M. Kahan, CFP®, president and senior financial planner of Financial Asset Management Corp., has nearly 30 years of experience as a financial planner. Kahan has committed a substantial amount of his time to the advancement of the profession. He served on the Financial Planning Association's National Board of Directors from 1997-2001; chaired a number of the organization's educational conferences; and served on the Leadership Development committee and the Practitioner Advisory Council. He currently serves on the Past President's Council for FPA of New York. He is also a member of the Editorial Advisory Board for the Journal of Financial Planning. Kahan has extensive media experience and also contributed to the books "So You Want to Be a Financial Planner, Inc. Yourself" and "The Encyclopedia of Financial Planning."

Roger Kruse, ChFC®, CFP®, EA
Founding Partner
FFP Wealth Management
FFPWealthManagement.com

Roger Kruse, ChFC®, CFP®, EA, a founding partner of FFP Wealth Management and a shareholder of National Advisors Trust, has been providing investment management, tax and financial planning advice for 25 years. His designations include Chartered Financial Consultant®, Certified Financial Planner Practitioner® and Enrolled Agent. Kruse is credited with developing the proprietary tax-planning tool, the TaxSuperSheet™, which is the cornerstone of the financial plans developed by FFP Wealth Management.

Wesley Stillman
Founder
RightSize Solutions, Inc.
Rightsize-Solutions.com

Wes Stillman established RightSize Solutions, Inc. in 2002 to provide cloud and virtual technology solutions to small- to mid-sized firms. He focuses on bringing together strategic partnerships in order to facilitate the promise of cloud technology in the Financial Services industry. Providing comprehensive IT Department services, he and his team help advisors gain greater flexibility, lower costs and increase productivity, with a laser focus on security and compliance.

Zohar Swain
President
Mink Hollow Advisors
MinkHollowAdvisors.com

Zohar Swaine is the founder of Mink Hollow Advisors, a boutique management consulting firm serving Wealth Management and FinTech. Prior to Mink Hollow Advisors, Swaine was responsible for leading the development of strategies, new product introductions, and the creation of value-added solutions with over 4,000 independent Registered Independent Advisors on the TD Ameritrade Institutional platform. His management consulting and executive position experiences span wealth management, retail banking, brokerage, and securities services.

Marie Swift
President and CEO
Impact Communications, Inc.
ImpactCommunications.org

Marie Swift is a nationally recognized consultant who has for over twenty years worked exclusively with some of the industry's top financial institutions, training organizations, investment advisory and financial planning firms. A top rated speaker at dozens of industry events, Marie is dedicated to elevating the conversation in the industry. Marie is also a prolific writer and contributes to many of the industry's leading publications, including *Financial Planning* magazine and *Money Management Executive*. A thought leader for thought leaders, she is known for bringing some of the industry's best and brightest voices together for dialog and debate. Her Thought Leader Roundtable series is just one example of how Marie generates interesting conversations with movers and shakers in the financial services industry.

This Thought Leader Roundtable was produced by:

IMPACT COMMUNICATIONS, INC.
Serving the financial services industry since 1993.

Questions about this transcript may be directed to Leesy Palmer, Director of Media Relations: (800) 974-7753 / ImpactMediaManager@ImpactCommunications.org