MARKETCURRENTS

WEALTH MANAGEMENT

TECHNOLOGY TRENDS

FAMILY OFFICE SERIES 2017

June 2017

MarketCurrents

The shift from bank financing to alternative lending has provided an unparalleled opportunity

Take advantage of this opportunity through Forefront

ForefrontCapitalAdvisors.com
888-484-4348
641 Lexington Ave, 29th Fl
New York, NY 10022

FOREFRONT CAPITAL

MarketCurrents LLC: Sumehr Sondhi (Publisher & Managing Director) MarketCurrents LLC, ssondhi@marketcurrents.co

Wendy Connett (Editorial Director) MarketCurrents Wealth Management
wconnett@marketcurrents.co

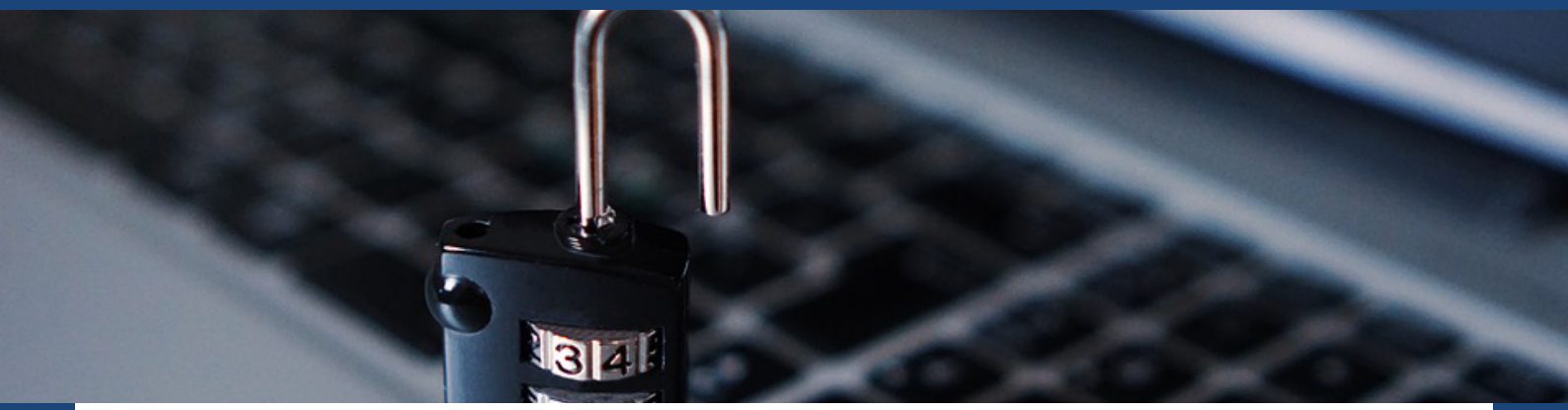
Vikram Kuriyan (Trustee) MarketCurrents LLC

7 Times Square, 37th Floor, New York, NY 10036, USA.
T: 1-917-960-8463. E: info@marketcurrents.co

Design: Version Next Digital Pvt. Ltd.

CONTENTS

EDITOR'S FOREWORD



As the nature and complexity of issues family offices face evolves, so does the technology that is needed to support them. The solutions used or sought are as diverse as the universe of family offices themselves. This can present significant challenges.

Of the four most important strategic challenges facing executives leading a single family office, enhancing operations through process or technology changes ranks the highest, according to a survey of single family offices conducted by Deloitte last year. Technology was also the most frequently cited unmet service gap.

In our second annual technology report, MarketCurrents Wealth Management delves into the role technology plays among family offices, the challenges they face, how to overcome them and the best practices involved in choosing a provider.

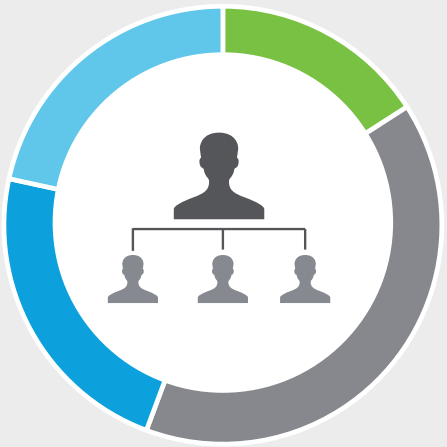
We also take a deep dive into cybersecurity, an increasing concern among family offices. Family offices said their biggest technology bet over the next three to five years will be IT security and infrastructure, the Deloitte survey found.

The experts we spoke to reveal who and what are the biggest threats and the steps family offices should take to thwart cybercriminals.

Finally, we bring you the highlights of a closed-door forum attended by family office execs and investors held earlier this month. Hosted by MarketCurrents, Tannenbaum Helpern Syracuse & Hirschtritt and Prime Alpha, topics discussed included why family offices are particularly vulnerable to cybercrimes and how to respond to a breach.

Challenges

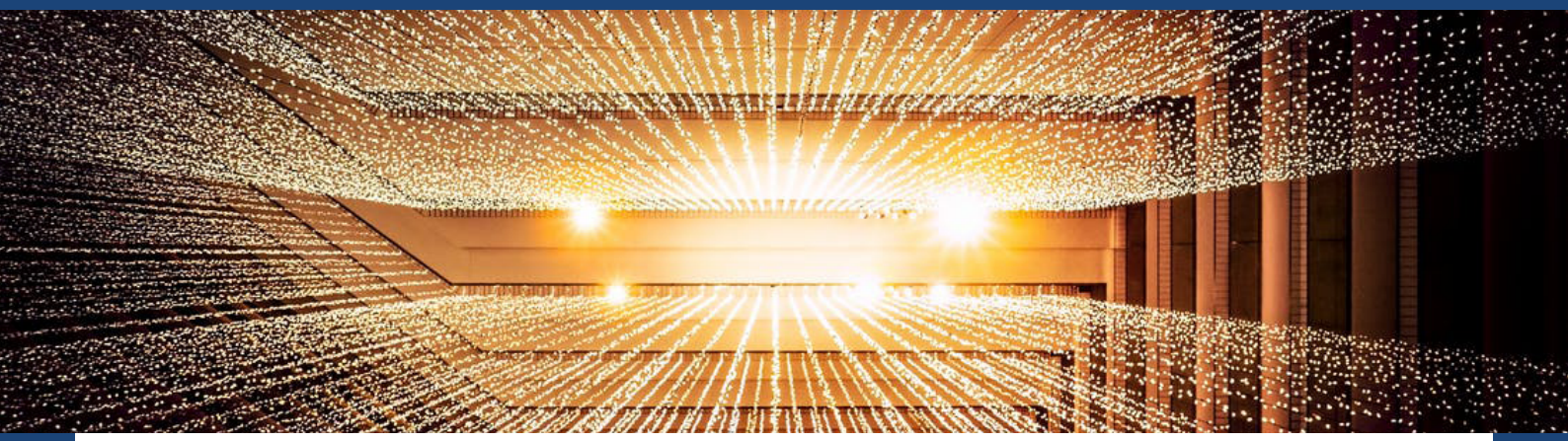
The four most important strategic challenges facing executives leading a single family office



- 35% Enhancing the operations of the office through process or technology changes
- 20% Understanding the true expectations of the family
- 19% Managing the investment returns and opportunities the family wants to pursue
- 14% Attracting, retaining, and motivating the right talent

Source: Deloitte Development

The Evolving Role of Technology



Edouard Thijssen, Co-Founder and CEO of Trusted Family, points out that single family offices typically function as an administration, coordination and services hub for a family. Some additionally act as an investment and reporting office.

Family offices need some basic infrastructure for handling documents and communication. Those that function as a reporting or investment office also need reporting, accounting and performance tracking infrastructure, he adds.

The role of technology has evolved in recent years due to a combination of the amount of data that needs to be processed, increased regulation and higher expectations in what family offices want, says Julia Cloud, Partner, Deloitte Tax LLP and National Leader of its Private Wealth practice.

Examples of the latter include a desire for daily portfolio performance reporting, versus monthly or quarterly, and instead of a hard copy being able to view it on tablets or smart phones, she adds.

In the last five years technology has evolved from focusing primarily on functionality and finding efficiencies to focusing on security, according to Theresa Pratt, Chief Information Security Officer at multi-family office Market Street Trust Company. “Technology has shifted from utilitarian to security,” she says. There is also more of an emphasis and need for training when it comes to social media and cyber risks, she adds.

The systems used by family offices range from Excel and QuickBooks to sophisticated platforms. The former, however, will not offer the checks and balances needed to tackle increasing compliance and regulatory requirements, Ms. Pratt maintains.

The New York State Department of Financial Services, for example, unveiled

the most stringent cybersecurity requirements in the U.S. earlier this year. They entail implementing cybersecurity programs and policies. One requirement involves audit trails with the ability to reconstruct financial transactions going back five years, Ms. Pratt explains. "How does Excel fit into that?" she asks.

Chris Martinez, Managing Director, Oakbrook Solutions' Family Office Practice, says the technology consulting firm is seeing more technology that tracks both sides of the balance sheet and non-marketable securities or illiquid assets including alternatives, such as hedge funds and private equity, direct investments, real estate, collectibles and artwork. Data aggregation technology is now allowing for the full range of assets to be included in a more holistic net worth statement. There is also an emergence of technology that allows for the customization of consolidated reporting, Mr. Martinez adds.

"Excel is still the most widely used program we see across the family offices we work with," he points out, but adds that more often than not it is no longer able to suit the increasingly complex needs they face.

This is starting to change rapidly due to increased regulations and risks, such as geopolitical, Mr. Martinez explains. The pace at which risks are accelerating has family offices asking what risks they are exposed to.

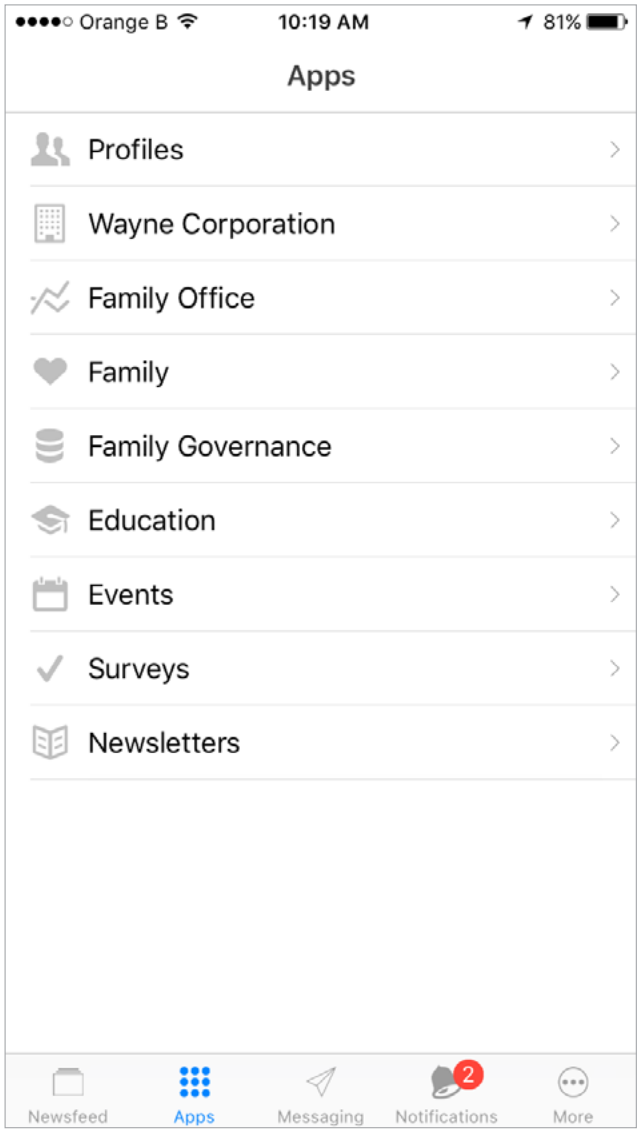
"The manual work and potential for error involved with Excel can no longer satisfy the needs of family offices," says Mr. Martinez. "Not only are more and better technology options available, families are seeing the value of getting that information in a more timely and efficient manner."

"The manual work and potential for error involved with Excel can no longer satisfy the needs of family offices."

Chris Martinez, Managing Director, Oakbrook Solutions' Family Office Practice

In addition, Mr. Martinez says to address privacy and cybersecurity concerns a number of secure and encrypted communication channels, such as secure family portals, have rolled out.

Mr. Thijssen, who has a technology background, is a next generation member of a multi-generational Belgian family office. He says he realized that once a family reaches the third generation, there is more family members spread out over different cities or countries and most don't have an active role in the office or operating business. Their ownership stakes start to vary.



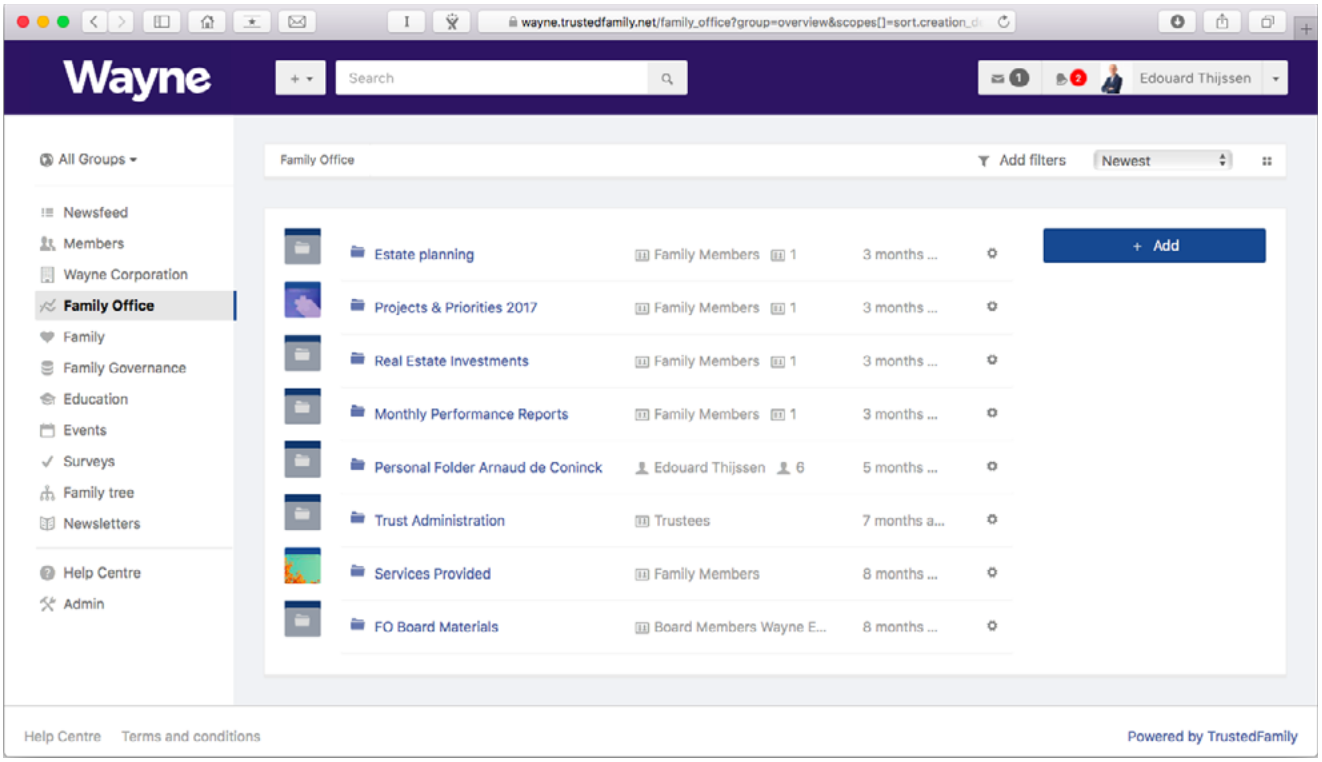
Source: Trusted Family iPhone App

He thought that transparency, good communication and centralization of all his family's important decisions and information were key to its long-term success. Along with a friend he built a platform to fulfill the needs of their own family offices. After building the platform other family offices and family businesses showed an interest, the impetus behind the launch of Trusted Family.

Trusted Family provides communication and document management in a centralized secure online environment that can be accessed from around the world. Documents can be shared and tracked and the right permissions can be set up for different family members, shareholders, directors and advisors who play different roles.

The platform can facilitate family and business governance as well as transparency among family members. They can also communicate from a single, secure platform and share anything from minutes of meetings, financial statements to business and family news. Finally, the platform can be used to organize meetings, run surveys and maintain a family tree.

It can also be accessed via an iPhone or iPad app and customized for each family. Each family office can set up customized groups and permissions, different topics and menu structures for the entities connected to the family and customize the look and feel with colors and a logo.



Source: Trusted Family Platform

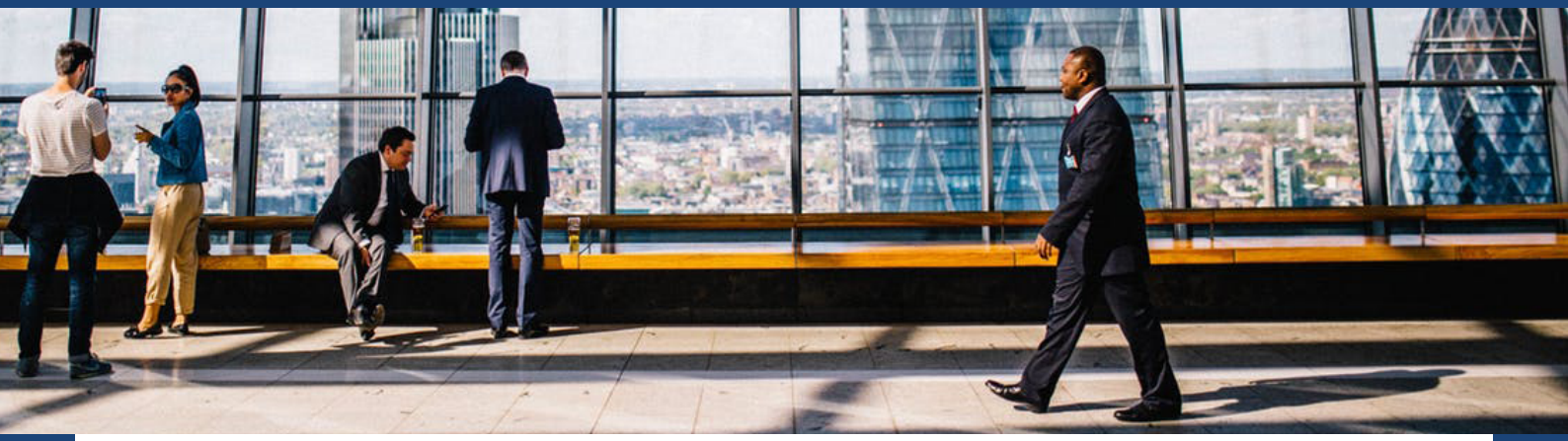
We believe that the alternative credit space has provided much needed diversification from the volatile equity markets

Take advantage of this opportunity through Forefront

ForefrontCapitalAdvisors.com
888-484-4348
641 Lexington Ave, 29th Fl
New York, NY 10022

FOREFRONT CAPITAL

Technology Challenges Family Offices Face



Among the operational challenges is the increasing complexity families face in regards to estate planning, wealth transfer, taxes and diversified investments, says Mr. Martinez. Adding to this is coordinating all interactions with outside advisors, such as those dealing with taxes, estate planning and investments.

In addition to outside advisors, the number and diversity of people involved in running a family office can present challenges, says Mr. Thijssen.

"What has always been a challenge is that family offices are very unique depending on the needs of the office. There is no singular technology solution," says Ms. Cloud.

Ms. Pratt points out that the platforms offered by providers are typically designed with banks in mind. "There isn't a solution that does what a family office needs exclusively," she says.

Another difficulty is that when moving data from one system or platform to another there can be inefficiencies,

"Secrecy and privacy is what families value a lot."

Edouard Thijssen,
Co-Founder and CEO of Trusted Family

slippage or human error, Ms. Cloud says. Family offices are still relatively small when it comes to the number of employees, which can also create hurdles, she adds.

Privacy is also an issue. “Secrecy and privacy is what families value a lot,” says Mr. Thijssen. But he points out that there is more often than not a lack of in-house expertise.

Source: Deloitte Development

Choosing a Provider: Best Practices

Family offices often face the age-old debate of whether to build or buy.

Building an in-house platform is more expensive and more difficult to maintain over time but can enable more customization than choosing an outside provider, Mr. Thijssen points out. On the other hand, outside vendors may provide a more robust platform that has the ability to evolve, he adds.

For those that choose to go the outside provider route there are many considerations, not to mention the number of potential pitfalls to be avoided.

"A common mistake is not having as full of a needs assessment in the beginning," says Ms. Cloud. This could mean that a family office didn't choose a solution that suits the most important issue they needed to address.

Ms. Pratt also maintains that when working with a third party, such as a vendor, family offices need to be clear about what they want to achieve. Some choose to work with consultants to help them navigate the myriad of platforms and providers, she adds.

A best practice is to clarify what problems a family office wants solved and what it wants to achieve and focus on vendors who specialize in the solutions needed, says Mr. Martinez. A platform built for a general partner of a hedge fund, for example, might not be suitable for a family that primarily manages philanthropic initiatives and foundations, he explains.

When working with a family Oakbrook starts with an assessment evaluating what technology is currently used and where the family is positioned. It then develops a three to five year strategic technology road map. Oakbrook also assesses how prepared they are to implement change over the next several years.

In addition to starting with the problems and challenges they are facing, Mr. Thijssen says that families should appoint one person to coordinate the effort. He also advocates that family offices talk to other family offices about their experiences.

It is very important to do a very thorough assessment of a vendor, says Ms. Cloud. Also key is making sure staff is properly trained, she adds. They might, for example, not know how to tap into the full capabilities of the platform being implemented.

"The biggest lesson we have learned from clients is to look at how ready a family office and staff are for change," says Mr. Martinez. It is also essential to understand how well equipped a vendor is to handle implementation. Things can go wrong because a family office or vendor lacked the appropriate staff to implement the technology, he adds.

Mr. Martinez says other pitfalls to avoid are goals that were not aligned between the two parties and current practices that are not able to support future goals. The latter can affect something as simple as moving from annual reporting cycles to monthly or quarterly.

Providers can be vetted in three ways, says Ms. Pratt. It is crucial to make sure they have the ability to deliver what the family office needs and that they will be able to so continuously and securely.

Strong project management is also key, according to Ms. Pratt. "IT projects are notorious for going over budget, over time and failing," she adds.

Once a platform is implemented it is also crucial to make sure that the vendor provides ongoing technology support, Ms. Cloud points out.

With new players constantly entering the scene, another good practice is to assess their longevity and to find technology partners with the ability to grow with the needs of a family office, Mr. Martinez says. He advises that family offices check references and that peer groups offer a good way to do so.

"A common mistake is not having as full of a needs assessment in the beginning."

Julia Cloud, Partner,
Deloitte Tax LLP, National Leader Private Wealth practice.

One **Premier** Cloud.
One **Complete IT** Platform.
One **Family Office** IT Partner.

EzeCastle INTEGRATION

In an ever changing technology and cyber risk landscape you need a technology provider you can trust!

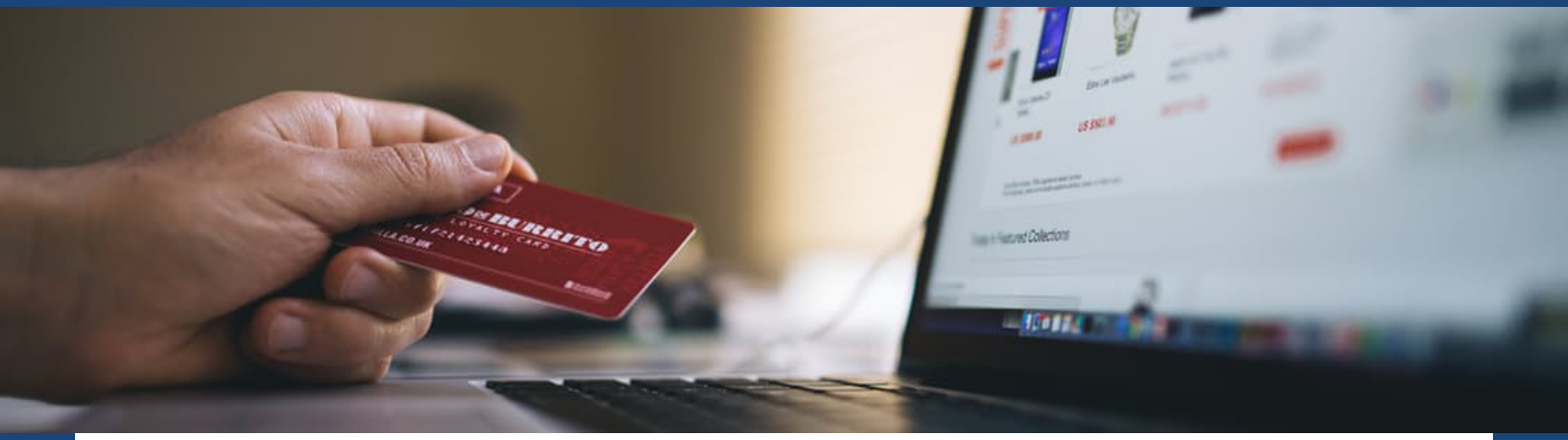
Eze Castle Integration is the leading provider of managed services and complete cloud solutions to over 650 investment firms, hedge funds and family offices worldwide.

- Complete Cloud Services
- Cybersecurity Protections
- Disaster Recovery
- Global Private Network
- Outsourced IT Support
- Voice Solutions

Contact us at 800 752 1382 (US) or 0207 071 6802 (UK)
Visit us at www.eci.com

LONDON | BOSTON | CHICAGO | DALLAS | HONG KONG | LOS ANGELES | MINNEAPOLIS
NEW YORK | SAN FRANCISCO | SINGAPORE | STAMFORD

Cybersecurity: The Threats and Risks



Cyberattacks are not only increasing in frequency and reach but also in their sophistication.

The recent WannaCry ransomware attack is just one example. WannaCry exploited vulnerability in Microsoft Windows. It infected more than 200,000 computers in approximately 150 countries and affected global companies including FedEx and government organizations such as the United Kingdom's National Health Service. The ransomware locked down all files on infected computers and the hackers demanded $300 in bitcoins to release them.

"The recent ransomware attack was unlike anything we have seen to date. The way in which it spread was pandemic," says David Niccolini, Executive Vice President and Co-Founder of TorchStone Global, a risk management and security firm specializing in family and corporate safety.

"While the world is becoming more sophisticated, the solutions are often rudimentary," adds Gary Raphael, Senior Consultant, TorchStone Global. He points to simply downloading a security patch that Microsoft provided two months prior to the WannaCry attack.

So who and what are the biggest threats? Cybersecurity threats can sometimes originate from the intelligence agencies of certain countries interested in obtaining information. Examples include China and Russia. "They are looking for information that they may or may not need and/or use one day," Mr. Niccolini explains.

Another is organized crime in Russia and parts of Eastern Europe, as well as countries that do not have extradition to the U.S., Mr. Niccolini adds. A third is individuals who operate on their own, often motivated by monetary gain or whom hold a personal grudge.

"If you think about terrorism, that landscape is no longer just physical it is now virtual," Mr. Raphael underscores.

One of the biggest mistakes a family can make is thinking that they don't have to worry about a cyberattack, TorchStone warns. Another is entrusting security to someone without doing the proper due diligence, Mr. Niccolini says. They may hire, for example, an IT professional whose experience is more "help desk" versus security.

Those families that have hired a qualified IT pro may find that they may just be so focused on the tech side of the security equation that the human aspects of security fall to the wayside, he adds.

"The weakest link in cybersecurity is the human element."

David Niccolini,
Executive Vice President and
Co-Founder of TorchStone Global.

The biggest threat to cybersecurity is human negligence. "The weakest link in cybersecurity is the human element. We see it over and over again," Mr. Niccolini says.

There are three major threats to cybersecurity, according to Ms. Pratt. "The biggest threat falls into the human realm," she says. Social engineering poses another major risk. "So many criminals out there are looking to trick you into giving away the keys to the kingdom," she adds.

In the realm of technology, social engineering occurs when cybercriminals use human interaction to get their intended victims to divulge sensitive information. An example is phishing, in which emails appear to be sent from a reputable source but in fact are designed to trick the recipient into clicking a link or attachment and sharing sensitive information such as passwords or credit card numbers.

The third major threat is not updating systems. Ms. Pratt also points to the recent WannaCry ransomware attack as an example of neglecting to update the patch rolled out by Microsoft.

"Negligence and lack of oversight are huge and underappreciated threats," says Michael Riela, Partner, Tannenbaum Helpern Syracuse & Hirschtritt.

While the news is filled with stories about data breach incidents involving outside hackers, a family office's own employees and vendors can also present a significant data security risk, he adds. They may steal information or they can simply act negligently, such as clicking a link and falling victim to a phishing or spear phishing scheme.

Spear phishing is a more sophisticated method of phishing and targets specific people or companies. Mr. Riela says an example of spear phishing is an email that appears to come from the CFO to wire transfer money but is in fact a fraud. "Once the money is out the door it's probably never coming back," he adds.

Many think cybersecurity is merely a technology issue, but it is actually a risk management and legal issue which require the attention of the board, management and legal counsel, Mr. Riela warns.

Too often clients believe the technology they have in place, firewalls and antivirus programs for example, will protect them. "There is no amount of technology that will completely eliminate risk," he says.

"So many criminals out there are looking to trick you into giving away the keys to the kingdom."

Theresa Pratt, Chief Information Security Officer, Market Street Trust Company.

Another common mistake is believing that cybersecurity insurance will cover all costs in the event of a breach, according to Mr. Riela. However, the cyber insurance market is not yet mature and these policies may not cover all costs, he adds. The language of a particular policy dictates what is and isn't covered, so it is important to review policy language very carefully.

Cheaper policies will cover relatively few types of costs. Those willing to spend some money on a cybersecurity policy can usually obtain coverage for items such as breach remediation, customer notification, public relations-related and legal costs, says Mr. Riela. However, the policy might not cover losses suffered in connection with the theft of intellectual property and will not cover the damage to reputation as a result of having suffered a data breach, he adds.

"Once the money is out the door, it's probably never coming back."

Michael Riela, Partner, Tannenbaum Helpern Syracuse & Hirschtritt.

Combating Cybercrimes

The best practice to thwart a cyberattack is to have a plan in place before disaster strikes, Mr. Niccolini says. Family offices should examine their information security as a cyberattacker would, says Mr. Raphael. This includes technical, physical and human vulnerabilities.

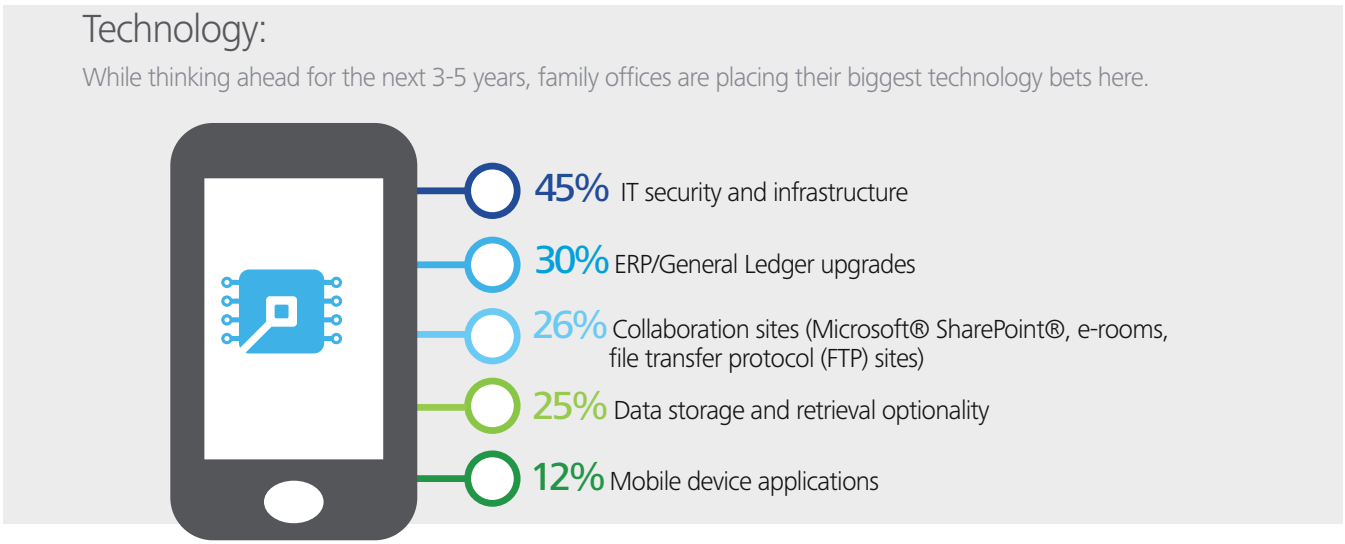
Education of family and staff is also a critical component of a plan. Education can prevent unintentional harmful acts, like being a victim of phishing, according to Mr. Raphael.

Ms. Pratt also sees education as key. Training should be conducted at all levels - from employees all the way up to senior execs and the board - as well as clients. Family offices should also make sure to keep systems up to date and to have more than one layer of security, she adds.

"More and more of the threats we see are related to phishing and social engineering coupled with weak passwords and free email accounts, such as Yahoo, which was compromised," says Mr. Martinez.

An increasing best practice among family offices is to set up corporate email accounts, which are more secure and can be centrally managed, he says. Secure password vaults are another good practice, he adds.

The first step is to perform a risk assessment, according to Mr. Riela. As part of the assessment, family offices should take inventory of the types of sensitive data they hold, such as Social Security numbers, account information and proprietary information on investments and deals. They should also determine where sensitive data is stored, including employees' home computers and mobile devices and how it can be accessed, he explains.



Source: Deloitte Development

In addition, family offices should consider who has access to sensitive data and who really should. Mr. Riela says that the only people who should have access to personally identifiable information and other sensitive data are those who have a reasonable need for it.

Ideally, Mr. Riela says, family offices should implement a data protection policy, which includes rules regarding what data should be encrypted, rules for using personal mobile devices for work purposes, a data retention and deletion policy, rules relating to downloading software, a password policy and a social media policy.

Family offices should also back up their data, preferably to a secure, off-site server, in case it suffers physical damage to its premises or if it falls victim to a ransomware attack.

Mr. Riela also maintains that it is important for the board and executives, as well as IT staff, to focus on data security and incident response planning. Family offices should consult with a data security attorney, who can help prepare for a data breach before one occurs and who can help respond to a breach, he adds.

It is also crucial for family offices to consider the data security practices of the funds and companies with whom they invest, such as hedge funds and private equity firms, according to Mr. Riela. When family offices perform due diligence on the recipients of their investments, cybersecurity should be a prominent part of the process, he adds.

Taking a Proactive Versus Reactive Approach: Q&A

In an interview with MarketCurrents, Matt Donahue, Business Continuity and Security Consultant and Steve Banda, Product Manager at Eze Castle Integration explain how organizations can better prepare against cyber threats.

What are the biggest cybersecurity threats investment management firms face?

There are constant threats facing organizations internally and externally, especially within the financial industry. One of the biggest issues is that the cyber threat landscape is continuously evolving. Hackers are trying to compromise firms in a number of ways – from phishing and social engineering to ransomware. It's becoming much like an arms race, where both sides (hackers and criminals vs. security firms and CISOs) are diligent, organized and well-funded, each gaining and losing the upper hand on a daily basis.

Steve Banda,

Founder, Product Manager,
Eze Castle Integration

Matt Donahue,

Business Continuity and Security Consultant,
Eze Castle Integration

From an internal perspective, threats emerge as a result of employees being inadequately trained, falling prey to social engineering scams or not following corporate policies. They also come from technology gaps including outdated IT systems, lack of patch management and other shortcomings that could have been addressed by vulnerability assessments.

Building on the importance of vulnerability assessments, firms should recognize that hackers are always scanning to identify holes and gaps that may provide an opportunity to breach an environment. This risk reinforces the importance of technology security defenses including next-generation firewalls, intrusion detection and prevention systems (IDS/IPS) and penetration testing. Ultimately firms want to close gaps and make IT environments unappealing to hackers.

Are there any key issues that family offices should be particularly mindful of in comparison to traditional asset managers?

Family offices must recognize cyber safety does not come automatically with obscurity, as all firms across the financial industry are potential targets based on the data they possess. When it comes to IT, family offices must be disciplined and commit to running institutional-grade operations. While this may sound like an insurmountable task, the reality is that cloud services and managed cyber security services make this both cost effective and attainable.

How can family offices prepare for increasingly sophisticated and invasive attacks like the recent WannaCry ransomware attack?

There are always going to be new and more sophisticated attacks, but firms should cover the basics. The recent WannaCry ransomware attack highlighted the importance of regular data backups, conducting patch management and having an incident response plan. It also demonstrated the dangers that relying on outdated and legacy technology can introduce into a firm.

Vulnerability assessments are also key to helping identify risks to minimize the potential for future situations.

What should be included in a cybersecurity plan?

There is no one-size-fits-all for a cybersecurity plan, but rather core components that must be included. A company's plan should be a living document that evolves with the organization and cyber trends. Firms should have an understanding of their most important systems and data as well as appropriate protections and access controls. They must ultimately identify what is most important to their business and protect those items.

Plans should have an incident response outline for rapid action, should a security incident occur. Response components should include communication procedures, including alerting service providers and regulatory agencies as appropriate. Lastly, employees need to understand that they are human safeguards, and their training is a critical component of a plan.

How does Eze Castle work with firms to put a plan in place?

While Eze Castle Integration's cybersecurity offering is comprehensive, we tailor our services to client needs. We work with clients to understand their cyber maturity and risk levels and devise an appropriate cybersecurity plan and program that aligns to immediate and long-term needs.

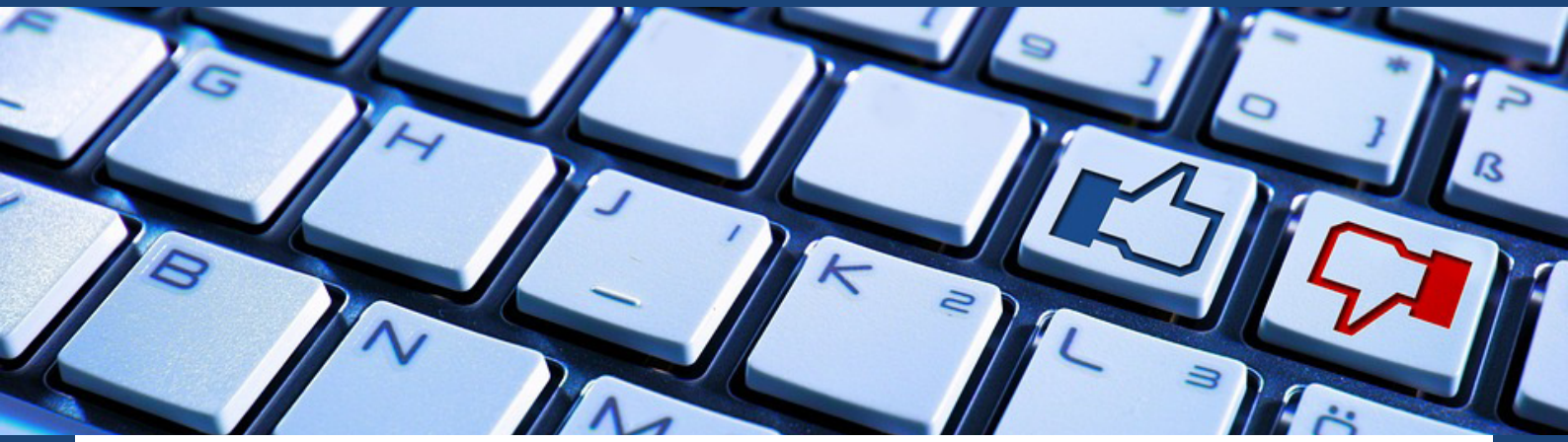
Our services include:

- Vulnerability Assessments and Penetration Testing Services which identify real and potential vulnerabilities that exist inside and external to a firm's network.
- Cybersecurity Plans and Programs cover creation, implementation, maintenance, and auditing of information security policies and plans.
- Active Threat Protection is a next-generation of managed cyber security solution, protecting hedge funds, private equity firms, and other financial organizations from advanced persistent threats.
- Simulated Phishing and Training is a fully-managed cybersecurity training solution provided by Eze Castle Integration.

What ongoing measures should be taken once a plan has been implemented?

Ongoing measures include testing and training, simulated phishing and online training. It is important for firms to conduct annual vulnerability assessments along with biannual penetration tests. Performing vulnerability assessments will allow firms to remediate risks identified through the risk assessment. They should also ensure patching is completed within a reasonable time period. With security ever changing, firms should be informed on risk trends, stay current on security threats or ensure their managed service provider is. Lastly, firms should implement security monitoring of the IT environment for ongoing, proactive protection.

Avoiding the Pitfalls of Social Media



Broadcasting sensitive information via social media can result in putting someone in peril as well as cause damage to reputation. Social media platforms can, for example, reveal the location of a user - valuable information for would be kidnappers. "There is a tendency for people not to view social media as a dynamic of the security playing field," says Mr. Raphael.

When working with families on social media best practices one of the biggest problems can be generational. "We are often called in by a patriarch who is worried by what their grandkids are doing. The kids come in rolling their eyes," says Mr. Niccolini.

TorchStone navigates family dynamics to come up with a solution with which both generations are comfortable.

"There is a tendency for people not to view social media as a dynamic of the security playing field."

Gary Raphael, Senior Consultant, TorchStone Global.

"Sometimes the fix isn't getting off Facebook," Mr. Niccolini explains. Instead it could be showing a family how to set the proper privacy settings.

TorchStone recommends the following social media best practices:

- Talk to children and teens about the apps they are using, the online relationships they have and cybersecurity risks.
- Make sure family members are tuned in to requests for sensitive information or displays of unusual behavior.
- Monitor a child or teenager's behavior in regards to online activity and review the public version of family members' social media accounts.
- Set the most conservative privacy settings, use strong passwords and only connect with those you know and trust.
- Use discretion when posting. Accounts can be hacked. Assume what is posted will be seen by everyone.

The Road Ahead

Mr. Thijssen sees a major shift among the next generation toward mobile applications.

Ms. Pratt has also observed the expectation by the younger generation for mobile technology. While older family members may be content with hard copies of quarterly statements, the next generation wants this information more frequently and delivered elegantly and seamlessly via a mobile device, she explains. “That’s a tall order,” she adds.

Another trend is robotic process automation (RPA), according to Ms. Cloud. RPA involves software with artificial intelligence, which automates tasks that are typically performed by humans.

This can help mitigate gaps that occur when moving data from one platform to another. The benefits of RPA also include the speed at which moving data takes place and that there is no room for human error, she adds.

There is also a migration toward cloud versus server-installed solutions, says Ms. Cloud.

The broadening acceptance of the Internet of Things will increasingly pose a risk to wealthy individuals, says Mr. Niccolini.

The Internet of Things, or IoT, is the connection to the internet of a wide variety devices, such as appliances and cars, which send and receive data. Connecting more devices in a seamless way makes a ransomware attack more likely and potentially more destructive, adds Mr. Raphael.

Mr. Riela says there is more sophistication regarding cybersecurity among investors. As part of the investment due diligence process, investors want to know how the recipient of their investments will protect their data.

PAMC

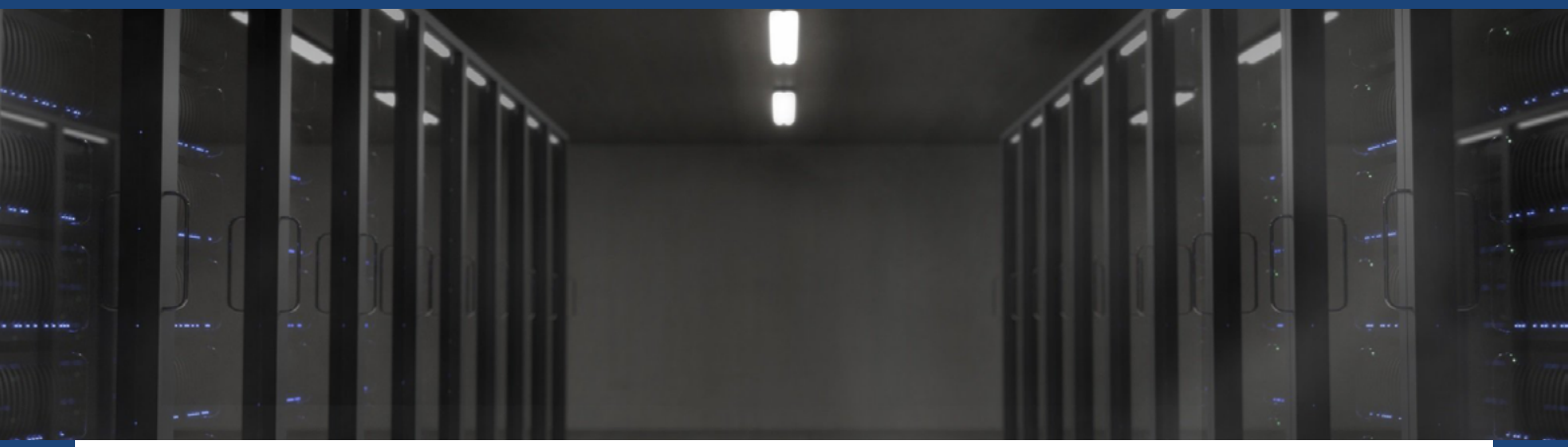
PAMC Is a collaborative partnership between MarketCurrents and PrimeAlpha

www.pamc.club

MARKETCURRENTS
WEALTH MANAGEMENT

PRIME ALPHA

KnowledgeForum: Common Issues and Data Breach Response Plan Essentials



Common cybersecurity issues unique to family offices and the key elements of an effective data breach incident response plan were just some of the topics discussed at an exclusive forum hosted by MarketCurrents, Tannenbaum Helpern Syracuse & Hirschtritt and Prime Alpha held at the Yale Club in New York City on June 1 and attended by family office execs and investors. What follows are some highlights of the discussion.

Mr. Riela of Tannenbaum pointed out that family offices are attractive targets to cyber criminals due to their wealth and the fact that many hold sensitive client information such as Social Security numbers and bank account information.

Family offices are also often generally softer targets than big banks who have technology and teams dedicated to cybersecurity.

Family offices that fall victim to a breach may also have to contend with bad publicity.

Forum participants said that it can be a challenge to get families to comply with security protocols and the extra steps they entail.

One participant pointed out that a good practice to avoid cybercrimes is to forgo online banking and stick to the old fashioned way – going to the bank in person. This is often a common practice in certain parts of Asia and Latin America.

Mr. Riela suggested that the following checklist should be included as part of a data breach response plan:

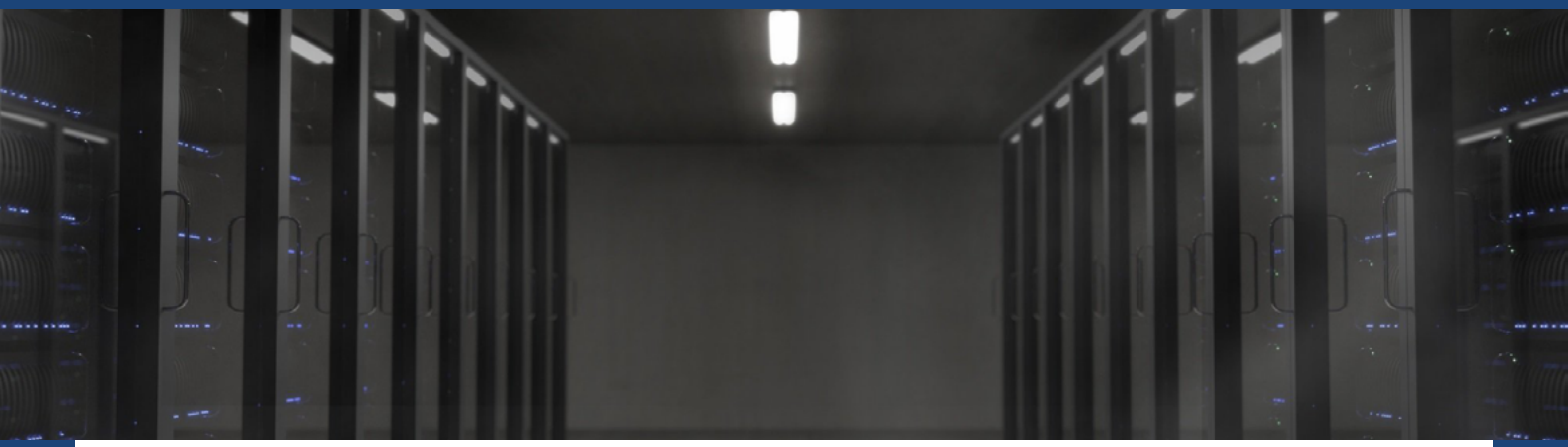
- Identify the breach response team. Who is in charge of doing what?
- Secure systems and make sure no additional data is lost.
- Notify cyber insurance carrier if a policy is held.
- Contact law enforcement.

- Notify bank and other financial institutions.
- Notify credit rating agencies.
- Manage internal and external communications. Determine who says what to whom, such as employees, clients and the media.
- Conduct a post mortem to determine what can be done better next time.

"There is going to be a next time unfortunately," Mr. Riela warned.

Source: KnowledgeForum 2017

Real Estate Investments and Family Offices: Q&A REI Equity Partners



Alan Blair, Managing Partner, REI Equity Partners discusses the intricacies of real estate investing.

Can you give us a brief introduction to REI?

REI is a fully integrated real estate investment, advisory, brokerage and management company. We are also an independent sponsor of risk-mitigated, long-term cash flow commercial real estate (CRE) investments with superior returns and an opportunity for capital appreciation.

Alan Blair, Managing,
Partner, REI Equity Partners

Since 2013, the core executive team at REI has refined a distinct strategy that leverages over 90 years of combined hands in experience and in depth understanding of acquiring and managing multi-tenant shopping centers. REI currently has over $30 million in assets under management.

A cornerstone of our strategy is our commitment to deliver unrivaled and exceptional service every day and in every transaction we have. Our fully integrated approach allows us to deliver the highest standard of excellence to our investors, clients and the communities where we invest.

What is your process for identifying suitable retail centers?

The identification process is where we bring value to the table. Our secret sauce is a combination of experience, a proprietary financial model, industry relationships, reputation and strict adherence to our acquisition criteria and strategy.

In 2010, we started a "buyer representation" CRE brokerage firm. In the ensuing years, we have been developing business relationships with most of the major CRE "listing brokers" around the United States. As a result of these relationships we receive most of the new for sale CRE listings from across the country, as well as many off-market listings. We filter through dozens and dozens of for sale listings every day. Once we see a potential property that we like, by inputting the details from the lease abstracts into our proprietary financial model, we can confidently project the cash flows for that retail center.

We do not rely on the marketing hype from the selling brokers. If the numbers can work, we then dig deeper into the local market:

-Is the micro economy growing?

-The demographics and employment figures.

-Who are the tenants and is their business "experiential" and recession resistant?

-Who are the shadow anchors? Are they financially sound?

If all looks good, we will then begin the price negotiations with the seller.

There is a lot of interest in real estate investing from family offices. What is the appeal to invest outside metro areas like New York?

A few facts before I answer your question directly:

-Family offices have many differing reasons for their interest in real estate investing.

-Many have extensive experience in real estate and people are always more comfortable investing in things that they know.

-Many others are simply aware that more wealth has been created over time from the real estate industry than from any other industry.

Most people invest in real estate in locations in which they are personally familiar, usually within a three-hour driving radius around where they live.

Many do not stop to realize that the real estate industry is not one industry. It consists of many very, very different sub industries and each requiring different skills and specialized knowledge in order to be successful. Take, for example, the differences between developing an apartment building from the ground up versus buying and

operating a hotel or developing and operating a golf course.

Think about the differences in risk, between buying raw land and building a shopping center, then appealing to the best national retailers in the country and negotiating the leases versus buying a retail center that is already stabilized and leased to the best retailers in the country. This complexity is multiplied by the thousands of geographic markets and sub markets, demographics and micro economies where the real estate is located.

All investment managers will allocate various proportions of their portfolio to different asset classes in order to maximize their returns and balance or hedge their risks. Depending upon the fundamental nature of the real estate investment, it fits only one of the many different asset classes or categories within the balanced portfolio. Some of the categories that could be a match with a real estate investment are:

-The high risk, high yield category/risk capital.

-The low risk, low yield, cash-flow/flight to safety category.

-The pride of ownership, generational/ blue chip category.

-The low risk, high yield, cash-flow/fixed income category.

So to answer your question directly: The reason to invest outside the metro areas such as NYC (or core markets) depends upon the reason and objective for investing in real estate and the category within the portfolio that the manager is trying to fill. The investment objective drives the decision. Within the metro areas and core markets, there is too much money chasing to few deals. As a result, there are literally no opportunities for low risk, high yield, cash-flow deals.

REI's fund objective is to offer a real estate product to fit the low risk, high yield, cash flow, or fixed-income portion of a portfolio.

REI identifies properties in affluent, secondary markets around the U.S. where we can still find opportunities to fit the low risk, high yield, cash-flow category. That, quite simply, is the appeal for those looking for an investment to fit that category.

What has historic past performance indicated about investing in shopping centers?

This is a much more difficult question to answer than one might imagine. Assuming we are talking about the type of shopping centers that we like to buy the answer is, it depends. It depends on whether the owner over paid and/ or over leveraged the acquisition at the peak of the market or not. Historic, national statistics will not tell the real story.

Fully stabilized, class-A centers with credit and national tenants are valued based upon the present value of the income stream generated by the rents. The value is higher the greater the confidence in the tenant's ability to continue to pay the rent.

The present value of the income stream determines the price. So to the extent you do not over pay for the income stream and the income stream is reliable over time, the performance is very predictable, in good times and bad times.

How could a family office go about investing in something like this?

Many large family offices will set up their own real estate acquisition or development team and keep everything in house.

Some other large family offices will "joint venture" partner with a real estate firm that specializes in the category of interest. When they joint venture, the family office will provide almost all the money and the real estate firm (partner) provides some money and all the expertise. In this way the family office will retain majority voting rights and decision-making authority over its partner.

Most family offices will be passive investors in public REITS or one of the larger real estate private equity firms. REI's fund is a smaller real estate private equity firm with a unique business model and investment objective.

How difficult or easy would it be for an international family office to invest?

Navigating the legal and U.S. tax code maze on your own would be a very complex and daunting task. But that is why we have taken the time to think this through with our legal counsel, who has extensive experience on this very point.

Basically, it requires that we set up an offshore feeder fund through which an international family office could invest and avoid the complexities and disadvantages of a direct U.S. investment.

Finding Alpha in a Volatile Market

FOREFRONT CAPITAL

Although the stock market has been successful over the past few years, a common theme has been volatility. Hedge funds have suffered their worst years in history due to their inability to time the market and find arbitrage in the changing world. Technology has ultimately changed day trading to quant trading and investment advisors are losing business to robo-advisors every day. The questions comes down to, how can one sufficiently invest in the ever changing, volatile marketplace?

At Forefront, we have realized that investors struggle to find arb, especially now, when investment choices are endless, technology is growing exponentially and no one knows where the market is going. Our answer is alternative credit. A non-correlated, trustworthy source of income, that can stand up to the volatility of the market, and provide a return stream attractive to all investors. Although alternative credit is a great space, the returns and the income come down to the investment manager, and the companies that can really differentiate themselves in a saturated market.

Forefront has realized the importance of differentiation and has created products and services that are really tailored to meet the investor's needs. Many alternative credit companies buy loans off the internet and package them for investors to invest in. This is a poor way of participating in the

credit space, as default rates are increasing as companies are lowering their lending criteria to underwrite more loans.

Rather than buying loans off of secondary sources, we originate and structure credit opportunities in-house, allowing us to control every aspect of the loan. We understand that risk is everything, especially in a volatile market, which is why we focus on risk mitigation, and ensure each investment has specific elements to mitigate risk and maximize potential returns. We only invest in small-mid size businesses that are undercapitalized, and are unable to receive a reasonable loan from a bank due to regulatory changes after Dodd Frank. We look to be at least two times over-collateralized and often use insurance and personal guarantee's to ensure timely repayment. Unlike the stock market, we understand what the worst case scenario is with these investments, and feel secure that with specific elements in place, even in the event of a default we will recoup the majority of our investment. Risk is the focus of Forefront, and we understand that investors need to feel secure even in a volatile, unpredictable market.

With the changing landscape on Wall St, investors need to search for arbitrage, and identify which companies offer the best investments to deal with the volatile and ever-changing market. Technology will provide more uncertainty than stability in the near future, and an investor needs to ensure to diversify into non-correlated asset classes to protect themselves from the changing world.

FOREFRONT CAPITAL

Contact Information:

7 Times Square, 37th Floor,
New York, NY 10036, USA.

E: *creifler@forefrontincometrust.com*

T: 212-488-4972

Digital Reports
Online Content
Events/Roundtables

and more...

MARKETCURRENTS

MARKETCURRENTS

WEALTH MANAGEMENT

MARKETCURRENTS

MARKETCURRENTS

WEALTH MANAGEMENT

Contact Us

7 Times Square, 37th Floor
New York, NY 10036, USA

info@marketcurrents.co

www.marketcurrentswealthmanagement.com

MarketCurrents

@currentsmarket