PAM
PRIVATE ASSET MANAGEMENT

NOVEMBER 2014
PAMMAGAZINE.COM
Protecting today's wealth for tomorrow

IN THIS ISSUE

TOP NEWS STORIES

SRI 'ATTRACTING WIDER INVESTOR DEMOGRAPHIC'

The type of HNWI interested in SRI has altered in recent years, *PAM* has learnt

TURN TO P4

SURVEY: MILLENNIALS DEMAND MORE ADVISOR TIME

Morgan Stanley and Campden Wealth research reveals next gen wealthy seek more contact

TURN TO P4

SINGLE FOs 'SEEKING MORE EXPOSURE'

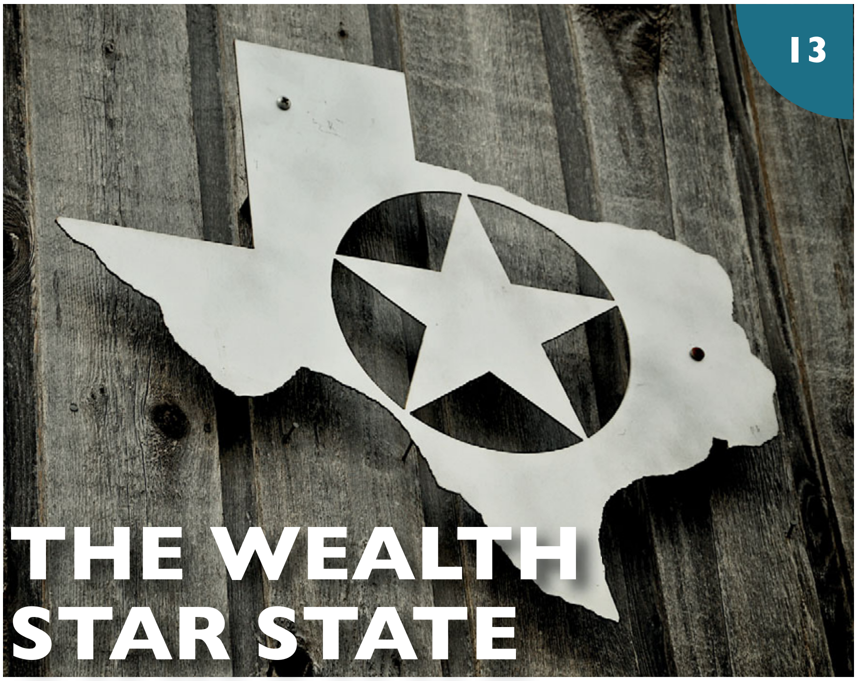
Single family offices are becoming more open, says Billionaire Family Office CEO

TURN TO P6

LOW INTEREST RATES RESULT IN COLLECTIONS BOOST

Rates shortfall gives way to HNWIs increasing valuables

TURN TO P6



13

THE WEALTH STAR STATE

PAM investigates Texas' private wealth market, and the growing needs of the state's affluent inhabitants

FEATURE

16

Securing the threat

PAM's latest breakfast panel focuses on mitigating the risks posed by cyber crime

COMMENT

21

Hedge fund strategies: to exit or embrace?

What affluent investors can learn from CalPERS' portfolio liquidation

FOR MORE INSIGHT SEE: PAMMAGAZINE.COM

Securing the threat

Coinciding with National Cyber Security Awareness month this October, the latest *PAM* breakfast panel took on the topic of cyber crime and discussed the ways in which affluent individuals can curb their vulnerability

BY STEPHANIE BARTUP

"Assume you will be the victim of cyber crime and mitigate the risks facing you as best as you possibly can" was the message to affluent families and individuals in the US at a recent *PAM* breakfast.

The topic of the event, 'Cyber Security Best Practice: A Guide for High-Net-Worth-Individuals and their Advisors', was discussed by panelists Christopher Falkenberg, president of Insite Security Inc, Glenn Siriano, principal, advisory – information protection at KPMG LLP, Edouard Thijssen, co-founder and head of Americas at TrustedFamily and Andrew Pitcairn, family governance council chair at Pitcairn Family Office.

From major corporations like Apple and eBay, to high-profile celebrities, it seems nobody is safe from cyber crime – and due to their status and the high-quality assets they have at stake, affluent individuals are becoming more frequent targets.

Christopher Falkenberg, president of Insite Security Inc

Glenn Siriano, principal, advisory – information protection at KPMG LLP

Edouard Thijssen, co-founder and head of Americas at TrustedFamily

Andrew Pitcairn, family governance council chair at Pitcairn Family Office

Discussing the ways in which HNWIs can mitigate the risk of being a victim of cybercrime from external threats, Falkenberg said making oneself as anonymous as possible would make a hacker's job more difficult. "Number one, you have to make it harder for these hackers to find out that members of single family offices are as affluent as they are," he said.

"This can be tricky; we have a number of clients listed on the Forbes list, for example, and so they're out there in the open as a very wealthy person. Once that happens, hackers will try to learn more – like where someone lives, who their employees are, where their kids go to school, and so on. That information can enable someone to launch an extortion plot."

Siriano gave an example of one attempted extortion of the CEO of a large corporation. "An email came into the CFO's office from the CEO's email stating they needed an urgent check cutting for a particular vendor. Unbeknown to the hacker, the CFO was with the CEO, so obviously knew it was fraudulent; but we see cases like this on a weekly basis," he said.

INSIDE THREAT

Siriano discussed the dangers posed by internal sources privy to a wealth of information, and warned that a threat could lie in the form of an employee at the private bank an affluent individual has an account with, or another organization close to the family.

"Some employees will look up HNWIs' bank account or credit card statements," he said. "They want to see what their holdings are – that's very private information. I'd say know your bankers, know what their security protocols are. Not only are there a lot of bad guys out on the internet, but they can be on the inside, too."

Siriano added that nowadays, affluent individuals aren't just affected by the companies that they entrust with their sensitive information, but also by the third parties that those firms might choose to outsource work to.

"In today's world, so much is outsourced to third parties, and those parties outsource to other companies. A lot of chief security officers are very concerned with this insider threat and data leakage," he added.

Internal threats might not only cause financial catastrophe, but reputational damage also.

Pitcairn gave an example of a large family-owned company that had to buy out a family member who took to social media platforms to voice her displeasure with the company operations. He told the audience that according to a study conducted by Privacy Rights Clearinghouse, over the past 10 years about 25% of security breaches were due to insider access or accidental disclosure.

He added that while his family office implemented controls around external hacking issues, he recognized that it was through internal procedures that the firm could have the most control and impact on educating employees about cyber security procedures.

"I know of one firm where system passwords were shouted between employees from one side of the room to the other – this is absolutely not best practice," he said. "There's always going to be ways to infiltrate a system from the outside, but make it as hard as you can for them; if you can mitigate internally you absolutely should."

Thijssen said hacking an affluent family would probably be surprisingly easy, as most members have never received security training.

"Many people are shocked by the amount of information that is available on the internet, through social media profiles and sites like Instagram for example," he says. "Many people 'geo tag' all the pictures and you can see very clearly where the next generation of wealthy teenagers are; what they do, where they go."

He added that once a hacker has a profile of the family, they will identify the weakest link – an individual whose online privacy settings are not set up correctly, for example – before sending a phishing email in order to try and gain access to sensitive data or passwords.

"Our view is that most of the mistakes that allow hackers entry don't come from technological errors, they come from human errors," he says. "Everyone relies on email today, but this is one of the most unsecure ways to communicate. I could send a link to someone through email asking them to register their details, and suddenly I have their information; and this has all been done without any technical knowledge."

> I'D SAY KNOW YOUR BANKERS, KNOW WHAT THEIR SECURITY PROTOCOLS ARE. NOT ONLY ARE THERE A LOT OF BAD GUYS OUT ON THE INTERNET, BUT THEY CAN BE ON THE INSIDE, TOO
>
> GLENN SIRIANO, KPMG LLP

Falkenberg agreed that the level of sophistication need not be high to cause serious damage. "It might not be low-tech stuff, but this is much more nuanced social engineering – like traditional fraud, or simply taking advantage of a situation, than really sophisticated hacking. This means that everyone is a potential target," he said.

TOP CYBER THREATS FACING AFFLUENT FAMILIES

THREAT	BEST PRACTICE SOLUTION
Email systems and password security	Don't click on any links or accept any files from unknown or potentially untrustworthy sources, and take advantage of additional security features offered with programs such as Gmail. Create memorable but unique passwords for each account, and keep this sensitive information between as few people as possible. Don't write the passwords down, and don't say them aloud in a crowded room.
Internal security breaches	Have a designated representative within the family who takes responsibility for cyber security, and ensure they hold frequent meetings to keep all relevant parties informed of any updates or changes which may affect the way online security is run in-house. Train all internal employees on the importance of effectively storing sensitive documentation and correctly identifying an individual before transferring funds or releasing data.
Social media and photosharing	Ensure the privacy settings on your social media accounts are set up correctly; leave as little information as possible in the public eye, and never reveal when you are on vacation, or where you are through photo 'geo tagging' to anyone but close friends and family.
Data storage	Make sure that all data is stored efficiently and safely. A limited number of people should have access to this sensitive documentation, and when possible, it should always be stored through an internal system.
Third-party employees and companies	When using third-party sources such as a private banking system or data warehouse, make sure you are aware of the company's internal policy relating to sensitive information. Be aware of who has access to your data, and limit to as few people as possible.

GROWING CHALLENGE

The issue of cyber security has become far more pronounced in the past couple of years given the huge amount of data available online. Siriano said that alongside internal and external fears, disruptive technology has also heightened the threat level.

"Everything can be accessed on a mobile device these days and this will continue," he said. "Disruptive technology is just going to explode over the next generation as cars have wireless capabilities, as will refrigerators and other household gadgets. You have to think about privacy regulations and implications – know what is attached to your network and whether you are securing it properly."

As new extortion techniques are created by hackers on a daily basis, mitigation rather than cure was the approach that the panel suggested should be taken by affluent individuals.

Falkenberg said that one need not provide a family office the protection you would see at a large government or national security enterprise, but simply make its online presence more difficult to penetrate by applying layers of security – much like the way we approach security in the physical world.

Thijssen suggested wealthy families should look at their security firewalls in the same way that they would at the physical walls protecting their physical assets.

"It's about building blocks and barriers to make it more difficult to get in compared to your neighbor," he said. “People don’t realize that with all these picture sharing tools these photos are saved forever. Additionally, using the two factor authentication security features on services like Gmail would stop thousands of these attacks – but people don’t set these up because they are cumbersome and require time to set up – thinking long-term though, these things need to be taken care of.”

Discussing the ways in which family offices were adapting to the growing cyber threats, Pitcairn said retaining as much control in-house over back office data and sensitive information as possible was key, adding that his family office had created its own data warehouse.

“It’s not for everybody,” he said. “It’s very expensive and takes a lot of technical knowledge, but being in control of your own data aggregation through your own infrastructure is vital for us.”

TAKING CONTROL

The idea of training family members and employees was also seen as a fundamental step by all of the panelists.

Thijssen suggested having one point of security contact in the family, who instigates a quarterly meeting for all family members or employees to discuss any developments in security practice which might affect the group.

“The family needs to decide what kind of information they want to protect, and choose where to store it; just creating a map of where that data is, be it spread over families’ email accounts or stored in online cloud systems, will help,” he said. “The risk mitigation process is never finished, you just have to integrate it as part of the culture.”

Falkenberg said training employees on the importance of data sensitivity and indemnity confirmation is just as important in the bid to create a secure family office.

“Administrative assistants, certain household staff, financial advisors – all of these roles are entirely driven by service; by people who want to make their clients happy,” he explained. “Hackers who have gleaned certain data or information can take advantage of this service mentality and may try to impersonate their employer. For example, if a financial manager receives an email requesting a wire transfer so their client can purchase a piece of artwork while on vacation, they might not consider that the email sender is not whom they claim to be.”

Falkenberg suggested a two-step verification protocol could be a solution to this situation. For example, requiring a phone call confirmation for wire transfer requests, rather than an easily impersonated email.

“Training is important not only for family members but also those in positions of trust who could be taken advantage of,” he added. “There is a huge cultural component to this problem.”

PROTECTING FAMILY WEALTH

- **70.8%** of family wealth firms say families are “moderately informed” about the everyday security risks they face, while **21%** are “insufficiently informed” and **4%** are “not informed at all”
- **29%** of households they serve have suffered financial fraud incidents
- **21%** of families served have reported incidents of burglary or robbery and **17%** have reported ID theft via email or internet
- **71%** of firms do not employ a security consultant

Source: The Family Wealth Alliance’s 2012 Inaugural Security Study Inaugural Security Study

> TRAINING IS IMPORTANT NOT ONLY FOR FAMILY MEMBERS BUT ALSO THOSE IN POSITIONS OF TRUST WHO COULD BE TAKEN ADVANTAGE OF. THERE IS A HUGE CULTURAL COMPONENT TO THIS PROBLEM
>
> CHRISTOPHER FALKENBERG, INSITE SECURITY INC

Siriano said that the movement is more focused on a multilayered security approach, and more proactive systems which focus on threat intelligence and vulnerability management.

“Assume you are going to be attacked or hacked; it’s not about prevention because you’ll never cover 100% of the possibilities; instead look at how you contain it,” he suggested. “Put more effort into the incident response and the containment so that you can stop it becoming a bigger issue.”

Pitcairn agreed there will always be some level of risk facing affluent families, but said education and the implementation of an effective checks and balance procedure will work as insurance, as will the ability to evolve with the industry.

“Our firm recently released an electronic device discussion guide to give parents, guardians and grandparents with younger children a resource to use when discussing expectations around security and usage,” he said. “Families face a lot of risk factors, especially on the mobile devices. It’s such a fast changing culture, we try to educate families and give them an opportunity to think about these risks from a family perspective.”

Discussing the kinds of systems affluent families could use to protect themselves, Thijssen said the idea of making technology platforms more secure while simultaneously making them easy to use would be considered by the technology industry for years to come.

“There’s a lot of people trying to build secure emails and encrypted email systems; I think that is where the industry needs to go,” he said. “There will always be a threat. As we work hard to mitigate against it, the hackers come up with new technology – it is constant cat and mouse.” ■