CRAIN CURRENCY

For families managing wealth and legacies.

WEDNESDAY, SEPTEMBER 28, 2022

VOL. 1, ISSUE 14

Cyber threats, from computer viruses to data breaches, are only becoming more sophisticated and more convenient for hackers. But are family offices adequately prepared, and have they taken the right steps to secure their wealth and data? Not really, Bailey McCann reports this week.

Also in this issue, we talked with Leslie Voth, CEO of the multifamily office Pitcairn, who was the first nonfamily member to take the reins — implementing some major changes and elevating the voices of women and the next generation.

We'd love to hear what you think of this newsletter — comments and concerns, story ideas, insights. Please forward your comments to Executive Editor Frederick Gabriel at fred.gabriel@crain.com or to me at marcus.baram@crain.com.

Marcus Baram

HANDPICKED

How family offices can prepare for next-level cyber threats

SHUTTERSTOCK

By BAILEY MCCANN

Given that the average North American family office has $1 billion in assets under management, it's no wonder these offices are increasingly attractive to cybercriminals.

In addition to financial repercussions, a serious data breach may expose family members to extortion, fraud and identity theft and even jeopardize their safety.

Still, many families are slow to take cybersecurity seriously.

"Families don't often invest in training for staff and family members on what we would call good cyber hygiene," said Bill Woodson, the West Palm Beach, Florida-based head of strategic wealth advisory and family enterprise services at Silicon Valley Bank. "And it can be difficult to engage with security companies because many of them are designed for corporate clients.

"As a result, these companies don't have a deep understanding of the family-office service model or the unique needs of families," said Woodson, who helps families manage business services within the office. "The services don't match up, the pricing models may not match up, so it can be challenging to bring in expertise before or immediately after an incident has happened."

For families that are trying to figure out where to begin, the family itself can do a few things in addition to searching for an in-house team:

- A data audit can help families understand where they are exposed, what levels of security protection already exist and what needs to be hardened.

- Family members can do basic things, such as use two-factor authentication, to add another layer of security.
- Professionals can help create a business continuity and response plan to help guide office staff when an incident does occur.

TOP CONCERN: FINANCIAL THREATS

Not surprisingly, financial threats top the list of concerns for families. Specifically, an insidious kind of wire-transfer fraud that results from a business email compromise. In this scenario, cyberthieves gain access to the private email of family members and monitor them for many months, learning how a family member writes any nicknames he or she might use or other details.

> *To prevent attacks, families have to train staff and family members on the basics, such as two-factor authentication and not sending sensitive details via email.*

Once the thieves learn those quirks, they can more convincingly pose as the other person, request wire transactions and direct those to bank accounts under their control.

“Business email compromise is one of the fastest-growing types of cybercrime in the world,” said Dr. Chris Pierson, CEO of Florida-based BlackCloak, a cybersecurity concierge for families, high-net-worth individuals and executives. “It can be difficult to track down where the compromise has occurred and for how long internal emails have been monitored by other parties. Then families have to figure out which transactions are involved and whether they can recover any of the losses.

“This can take time, and if you authorized the transaction, the bank isn’t really responsible for reversing it. So it’s a huge pain point for families.”

Kenneth Rashbaum, a New York-based partner at the law firm Barton LLP, agrees.

Rashbaum, who helps families understand cyber risks, said that to prevent attacks, families have to train staff and family members on the basics, such as two-factor authentication and not sending sensitive details via email.

“It may be worth going to good old-fashioned voice communication,” he said. “Banks might do this where they call to verify a transfer, but families should be proactive about this and call in transfers, whether that’s to an office member or another institution. A lot of these guys monitor email boxes for words like ‘wire’ or ‘ACH.’ And if those don’t make it into an email, then they aren’t going to get picked up.”

MAKING BACKUP PLANS

Apart from training family members and staff on what to watch for, family offices also need to have a formalized backup plan in place if an attack occurs. This is commonly known as a business continuity plan and should include procedures for restoring information, dealing with ransomware and securing operations after an attack.

A continuity plan not only is necessary to have in general but also can help families qualify for cybersecurity insurance, said Tiffany Garcia, a director and national cybersecurity practice leader at CBIZ Risk & Advisory Services, a global professional services provider.

Cybersecurity insurance is still new but is a growing area of coverage and can help with the costs of recovery after an attack. However, policies aren't typically available unless an organization can prove that it has strong cybersecurity practices and a business continuity plan in place.

"These policies are typically very expensive already, and it's getting harder to get them because attacks are increasing," Garcia said. "Families that qualify will have to look closely to determine if the coverage is worth it. If you don't have a good cybersecurity plan, your premiums could be very high, and the policy may not cover much.

"Families may also determine that it makes more sense to self-insure. However they do it, looking at coverage options and requirements can be a good tabletop exercise for families so that they can see where their cybersecurity efforts stack up."