SPOT

An expert weighs in.

Jordan Arnold, K2 Intelligence Managing Director and head of Private Client Services.

As told to George Chang

LIGHT

Inside Threat

Q. How do you minimize vulnerabilities associated with hiring staff and advisors?

The reality is, the people you let closest to you are best positioned to exploit you. Proper due diligence and research is critical to security. For example, it is standard procedure to conduct a home inspection prior to buying a property to assess its value and risks. It should also be standard procedure to assess the backgrounds of those who work in your home and with your critical assets. It means not hiring the CPA who, unbeknownst to your friend who recommended her, has a history of judgments, liens and lawsuits. It means doing periodic background checks on household staff, so you learn about an employee's recent arrest before he can endanger your family. The expense of preventing a problem is always less costly—financially, reputationally and otherwise—than dealing with one.

We are seeing more awareness that threats often come from the inside, and are helping our clients conduct the appropriate level of due diligence to meet their needs. When an unfortunate event does occur, we respond to it, contain the damage and take whatever action is necessary, including referrals to our former colleagues in law enforcement.

Cyber

Q. *What can individuals do to protect themselves from cyber crimes?*

Cyber crime against high net worth families is on the rise for various reasons: 1. Potential financial rewards are greater. 2. High net worth family members have more people/staff handling personal emails and finances. This increases the risk that someone will make an error or leave a virtual door open to let cyber criminals into a private network or bank account. 3. Many of these families are high profile and therefore more vulnerable. Cyber criminals are spending the time to get to know their targets. By breaking into networks and using publicly available social media, the bad guys are able to learn about where you travel, who you trust and how you conduct your communications and personal business.

Cyber criminals are constantly upping their game: that unsubscribe link in what appears to be a random spam email could actually be a targeted attack—you click it and within 24 hours you're being extorted…financial payment demanded in exchange for the non-publication of your now-stolen personal photos and financial documents.

K2 Intelligence is offering a tailored service to help families raise their cyber defenses through hands-on assistance and education. Our team of experts will visit a home to assess and strengthen the security of all personal devices including computers, tablets, smartphones and internet connections used by the client, immediate family members and personal or executive assistants. We also provide training to make sure the family understands how to protect themselves from this kind of crime. Awareness is key to defense.

Art Risks

Q. *What are some solutions/strategies to protect investments in art?*

Art is bought and sold in what remains the world's largest unregulated marketplace. Works routinely sell for more than the average cost of a home and transactions are frequently conducted from afar. You have crooked dealers selling encumbered, stolen or even counterfeit works; sanctioned parties and criminals laundering funds through highly portable paintings; and the modern graphic designer's toolkit in the hands of a forger is like a license to fake everything from provenance documents to the works themselves. Collectors need to evaluate not just the authenticity of what they're buying, but who they're buying from. It's also critically important to conduct routine, documented audits of a collection, especially when works are held in storage or displayed in different locations—the odds of solving a theft is typically a function of the amount of time that passes between the taking and the discovery.

Travel Security

Q. *Given the increase in terrorism risks, what are your recommendations for travel security?*

First and foremost, you need to get smart about where you're going, and plan accordingly. Obtaining a travel security brief will provide you with a risk assessment of the country you're visiting and highlight specific safety and logistical considerations as you prepare for your trip. Emergencies will happen, and for that reason, it's critically important to set up points of contact for your family and travel partners, obtain contact information for the US Embassy or Consulate, and know how to obtain proper medical and/or evacuation help if necessary. Other things to keep in mind: know the local laws and customs (so as not to run afoul of them); bring clean electronic devices with you and be careful how you connect to the Internet; only use official transportation providers (to reduce kidnapping risk); and don't speak carelessly about yourself or others in public spaces—you never know who is listening and how they might use that information. For those travelling frequently or with large family groups, the use of outside providers can quietly provide reassurance that you are prepared and will minimize the risks during a crisis.

Philanthropy

Q. *How do you protect the integrity of philanthropic efforts against possible theft or compliance risks?*

Your generous charitable contributions should go to their intended recipients, and not into the hands of fraudsters or those with a history of irresponsible stewardship. We are routinely asked to vet non-profits and individual fundraisers to ensure that an investment in a worthy cause is also a "good investment." As part of this assessment, it's essential to confirm that your sensitive financial and related personal information is being handled with the appropriate controls in place and that all relevant laws and regulations are being followed. **LM**