

Fear Factor

Investment Opportunities Born of Our Aversion to Risk

By Bart Schachter and David Frankel, Blueprint Ventures

OCTOBER 2005 - For centuries, societies have been evolving how they manage risk. Every day, it seems that modern life bestows upon us new manifestations of risk that deserve to be addressed. Natural phenomena like hurricanes, earthquakes and floods have been with us forever. Technology routinely brings us new risks: automobile accidents, nuclear fallout, computer viruses and identity theft to name just a few. And social and cultural forces have created wars and terrorism. To the entrepreneur and to the venture capitalist, each of these is not a risk, but a business opportunity.

As an investment genre, risk mitigation offers some particularly interesting nuances. We were all taught that ulti-



mately, the market is perfectly rational and that any behavior to the contrary is a short-term anomaly. But modern humans have shown a consistent propensity to spend disproportionately when it comes to managing certain kinds of risks.

This is thanks in no small part to the news media. Terrorism, cyberterrorism, natural disasters, and other crises weigh heavily in the minds of many, and are creating or enhancing investing opportunities at all points on the scale, including venture. One or two isolated events are all it takes to launch a new risk-mitigation category, and once established, a periodic "renewal" event keeps the risk alive.

Ticket to Ride

We've made lots of progress with automobile safety, using cost-effective solutions like seat belts. But as we strive to make incremental improvements, our efforts may be less fiscally defensible. Child safety seats were mandated by law some decades ago, and they certainly help prevent deaths and injuries to kids – but at hundreds of dollars per seat and millions of seats deployed, the math suggests there might be other ways to spend those dollars that would provide more benefits to children. Airbags are a similar story, especially as we've evolved from driver airbags, to passenger systems, to side and headliner systems.

Today, we spend money to install an airbag, and then to automatically disable it (when an underweight passenger is in the "protected" seat). We've invented a risk-mitigation technology that carries its own risks in need of mitigation (not a unique circumstance).

Several years ago, a handful of automobile accidents were traced to a particular vehicle design that was prone to rollover when the tires weren't properly inflated. This led to great video and plenty of news coverage. Technology had the answer in the form of built-in tire-pressure sensors that could alert the vehicle operator at the first hint of improper inflation – and with a few more transistors, we can even prevent the vehicle from being started (or, with GPS, from being driven in anything other than a direct path to the nearest air compressor). With a little regulatory effort on the part of the US National Highway Transportation Safety Administration, a new industry was born, and venture investors that are funding the sensing, communicating, and displaying of this data will likely be rewarded when the mandate to include this feature on every vehicle kicks in later this decade.

Fear of Flying

For some reason, transportation provides seemingly countless examples of irrational risk assessment. Commercial aircraft offer the safest way to get from here to there, and yet a sizable fraction of our population suffers from a fear of flying. Layer in terrorism and the preoccupation with risk goes into overdrive. Worldwide, there have been a few documented attempts by (presumed) terrorists to shoot down large aircraft using black-market (Ebay?) surface-to-air missiles. So around the world, governments, airlines, military contractors and others are developing "countermeasures" to stave off the threat. A Rand Corporation study suggested that equipping the US fleet of 6,800 airliners with such systems might carry an initial cost of \$11 billion, and cost \$2 billion annually in on-going expenditures. If such a system prevented one 767 from being shot down every three years, the cost per EACH life saved would be about \$20 million, excluding the initial \$11 billion. The US Homeland Security Department is already working on tests with several aircraft.

Why are people afraid of flying, anyway? In their book "Freakonomics," authors Steven D. Levitt and Stephen J. Dubner reference risk consultant Peter Sandman, who explains, "Risks that you control are much less a source of outrage than risks that are out of your control." This, they suggest, "might also explain why most people are more scared of flying in an airplane than driving a car. Their thinking goes like this: since I control the car, I am the one keeping myself safe; since I have no control over the airplane, I am at the mercy of myriad external factors."

Technology greatly enhances our ability to sense, identify, and communicate and respond to what is happening around us – and thus offers a host of opportunities to address people's fears.

So whether it's supported by the probability assessments or not, we're likely to see this kind of spending continue.

The Camera Eye

Last year, we invested in Vidient. The company was an early-stage corporate IP spin-out of NEC. Their application suite analyzes video from a closed-circuit TV system. It recognizes objects, tracks them frame-to-frame, and identifies and alarms on targeted behaviors. Several airports are using Vidient to alert officials when somebody tries to go the wrong way in a security checkpoint exit lane (even among a sea of people going the "right" direction), or when an intruder grabs a secure door just before it latches after an authorized, badge-carrying individual has passed through. Vidient can sound an alarm, lock down a gate, or send a video clip to a security officer virtually instantaneously, potentially averting disaster.

Thanks again to recent events and the media, opportunities with subway systems in London and New York are now turning into Vidient purchase orders. Most of these venues already have the video infrastructure installed – SFO has well over a thousand cameras, and the Tube has at least five times that many.

Previously, the images were recorded and, after the fact, could be analyzed to reconstruct a disaster. The Vidient software delivers a real-time reaction. What security official wouldn't be attracted to that level of control?

Keep Secrets

The fear factor is paying off nicely in other sectors of our investing arena. The Internet has invented numerous industries, and cybercrime is now thriving. Viruses are now a mature industry – almost as quickly as Microsoft can put a security hole in one of its operating systems, the hacker underground will exploit it, and an entire industry of virus prevention specialists– which has spawned some notable IPOs – goes to work to quash it.

Now we have spyware, denial-of-service attacks, phishing, identity theft, and more – each an industry in itself.

In Blueprint's own portfolio, embedded software specialist Teja delivers intrusion detection technology as part of its multicore CPU suite.

Another of our portfolio companies, AirTight Networks, builds systems that address wireless security for corporate IT managers. Corporate infoworkers are clamoring for the convenience of wireless access – so much so, that they sometimes install their own access points under their desks.

But these "rogue" portals, as well as a host of other wireless vulnerabilities, create huge holes in the corporate network fortress. What CIO wants to be on duty when corporate proprietary data starts leaking out like water through a broken levee? AirTight to the rescue, with technology that not only detects, but intercepts such hazards.

When looking at entrepreneurs' business plans, we always ask, "What problem are you trying to solve, and is the market big enough to support a sizable business?"

The great thing about many of these risks, and risk mitigation techniques, is that they create their own markets. Even if an organization has never suffered from a denial-of-service attack, it's still subject to the RISK of such an attack. And once a deployable solution has been invented, wouldn't it be irresponsible for an IT manager to fail to deploy it?

Theft of personal information rarely happens, but when it does, again, it makes for great headlines. The media fans the flames. With 535 lawmakers all looking for a cause, we quickly get laws like the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act, mandating information security in health-care and finance, respectively, and spawning a slew of start-ups.

Is this fear rational? Probably not all of it. But we plan to profit from it.

Bart Schachter and David Frankel are managing directors with Blueprint Ventures. Schachter focuses on comm. and IT infrastructure, wireless technologies,

nanoelectronics, software and comm. semiconductors. Frankel focuses on semiconductors, systems, software development, and high performance computing and IT infrastructure. They may be reached at bart@blueprintventures.com or david@blueprintventures.com.