Cybercrime: The Single Biggest Threat to Your Wealth

By Brad Deflin

THE cybersecurity business provides a front-row seat for what's happening in the world of hacking and cybercrime.

For us, the operating arena isn't about servers, LAN cables and databases. It's about Windows, Macs, Android, Apple iPhones and iPads. Our operating experience is where the rubber hits the road in cyber threats today. As a result, we have a distinct finger on the pulse of what hackers are doing and where the action is heading.

Since the second half of 2017, we have seen an accelerating trend that I want to bring to the attention of *Bauman Letter* readers. But first I need to provide some context.

The No. 1 Problem for Mankind

Before starting Total Digital Security in 2013, I spent 25 years advising some of the wealthiest families in the world. I was a senior executive with Wall Street's most prestigious banks. For my ultra-wealthy clients and me, it was all about risk management and mitigation.

We were relentless in asking ourselves what could go wrong and how to avoid it. When facing the question in early 2012, we received a new answer. It would challenge every assumption we had ever held about our job.

In the early 2000s, targets expanded from big governments and Fortune 500 companies to include mid-sized companies. And, the attacks and incident rates showed more than the traditional sort of cyber-espionage. The hackers' goal was financial gain.

Around 2010, smartphones and cloud computing drove cyber risk toward smaller targets. The new cybercrime-for-profit attacks included small businesses and professional practices.

This time, the perpetrators weren't only black hats, but professional criminals and amateurs.

Cybercrime became job No. 1 for crime cartels, organized hacking syndicates and even disaffected street thugs around the world.

It was shocking at the time how quickly it happened. From a slow start in the 2000s, cybercrime-for-profit accounted for more than half of all cyber attacks around the world by 2013.

The pattern continued, and, by 2016, law enforcement in the U.K. declared that cybercrime accounted for more than half of all crime in the country.

In 2017, at Warren Buffet's annual Berkshire shareholder love-fest in Omaha, when asked about risk in the world, Buffet replied: "Cyber, it's the No. 1 problem for mankind."

Mr. Buffet went on to clarify that, in his view, cyber risk posed a greater threat to man than nuclear and biological weapons. If that doesn't punctuate the internet's democratizing effect on cyber risk, I'm not sure what does.

You're Retirement Years at Risk

Today, cybercriminals are targeting broader economic classes. They are aiming at the mass-affluent and upper-middle-class.

In the business sectors, targets continue to move downstream in size. If you engage with information and technology, you are a target of cybercriminals from around the world.

Here's what a sampling of what looks like in the real world from recent cases we've handled:

- $95,000 lost by a recently retired couple while buying a downsized home for their golden years with an agent using "free" email.
- A funeral home owned and managed by family members stalked and harassed by a disgruntled former employee.
- Multiple online investment accounts breached

and wiped out, including an individual that lost everything from three separate investment firms.

- Over $40,000 lost by a "man-in-the-middle" exploit on a small business, and then another $34,000 pilfered while they were trying to figure out what happened.
- A divorcee's life made miserable by an ex- that found a hacker-for-hire on the internet to disrupt every aspect of her daily existence.
- An accountant, operating the practice without any cyber protection whatsoever, lost client records for use in ID theft and IRS tax-refund fraud.

The list goes on. Some stories and cases are heartbreaking. It's important to know that the potential damage to you is severe.

Here are five crucial takeaways from these experiences:

1. All of the breaches took place on personal technology — no servers, LAN rooms or databases involved.
2. The majority of cases begin with information stolen from computers and laptops used at home.
3. The victims, when not a small business, were affluent upper middle-class individuals or families.
4. Three-quarters of the victims are retirees.
5. All of the exploits started with unsecured and "free" email accounts.

For the couple that lost $95,000, it started with a hacked Gmail account used by the agent during sales and closing. The client's lawyer is considering a suit against the agent and broker for not taking reasonable protection measures.

For the individual that lost multiple investment accounts, her email account had been hacked. The criminals were following her activities for weeks, if not months, before the breach.

Hacking and cybercrime are increasingly a threat to mainstream life. It's going to get worse before regulation and law enforcement counter the wave risk we have immediately at hand.

Don't Wait to Safeguard Your Data

The good news? There are steps you can take to reduce risk, reduce your digital footprint and make you less of a target.

First, be sure your network of advisers is taking your privacy and information security seriously.

If a real estate agent, CPA or any other "trusted client advisor" is using "free" email such as Gmail, Yahoo, AOL and the like, they are not with the times. Either give them a last-chance ultimatum to adapt, or fire them.

If they haven't made the effort to privatize email communications by now, you have to wonder how they value of your relationship.

Second, privatize your email accounts. Remember, cyber-attacks today start by targeting people, not IT departments. Privatizing email gets you off the grid of abuse and is a fundamental adjustment.

We create personal and business email domains for clients all the time; it's one of the "fundamentals" we discuss in every case. Your information's value will only increase in time, as will the added digital autonomy it provides.

Another fundamental for risk management today is to protect your home network. It's the port-of-entry to your life. Take control of your network like it was the main gate to your kingdom, because in the digital age … it is.

There are remarkably effective solutions with "set-it-and-forget-it" simplicity. These solutions operate with the effectiveness of "an IT security department in the basement."

From a best-practices standpoint, it's time to manage passwords, use two-factor authentication, freeze credit files and use a VPN. Many of these are inexpensive or free. You can visit http://www.totaldigitalsecurity.com for everything you need around these measures.

Back in my banking days, I recall when advising clients to take certain measures to reduce risks garnered the response: "How much will it cost?"

Answering that question is simple. There is no greater economic value than using advanced cybersecurity technology to protect yourself from loss and damage.

Use it and find yourself and those you care about most empowered for survival and success in the new digital age.

You can email me for more information at mailto:brad@totaldgitalsecurity.com. ■

Brad Deflin is a seasoned business executive with success at both the large corporate level, and in the pioneering of start-up companies. Brad co-founded Total Digital Security. Contact Brad at Brad@TotalDigitalSecurity.com.