KELLY FINANCIAL SERVICES LLC

Cybersecurity: Self-Awareness for Your Self-Protection

By James P. Freeman

"Attackers may set their sights on large industrial plants, factory floors, traffic signs and transit systems, and shut down banking systems."

– Frank Abagnale Jr. (*Scam Me If You Can: Simple Strategies to Outsmart Today's Rip-Off Artists*, 2019)

While the film "Catch Me If You Can" (2002) took some liberties with his life story, Frank Abagnale Jr. did pose as an airline pilot, a doctor, a lawyer, a Federal Bureau of Investigation (FBI) agent -- and other roles as a wily impostor -- all between the ages of 15 to 21. Later, he served a prison sentence for cashing $2.5 million in forged checks in 27 countries during his criminal years. But Abagnale left the dark side.

His imprisonment was reduced (from 12 to 4 years) by his becoming an unpaid consultant to the FBI. And he subsequently founded Abagnale & Associates. The firm advises on fraud prevention. Its clients include financial institutions, large corporations, and law enforcement agencies. Today, Abagnale teaches at the FBI academy and is an ambassador to AARP's Fraud Watch Network. He is recognized as one of the world's most respected authorities on forgery, embezzlement, and secure documents. And he has some ideas about the growing menace of cybercrime.

Abagnale told thinkadvisor.com in 2019, "You have to be a smarter consumer and wiser businessperson today."

Cybersecurity is back in the headlines again.

On May 7, 2021, Colonial Pipeline, an American oil pipeline system that includes storage facilities, suffered a ransomware cyberattack. The ensuing criminal act forced the shutdown of one of the largest pipelines in the U.S. -- carrying 45 percent of the East coast's fuel supplies and

running 5,500 miles, which transports gasoline, diesel fuel, and jet fuel from Texas, running up the East coast to as far away as New York -- in an effort to contain the breach of its computer network. Like every business today, computers run Colonial's operations. And like any command and control system that relies on the internet, such communication and information are vulnerable to nefarious activity. The result of this particular hack?

Chaos.

National media reported gas shortages, panic buying and price gouging. And The Wall Street Journal reported that the company agreed to pay $4.4 million dollars to the hackers (purportedly a group called Darkside) who sent the company software to effectively unlock and regain control of its systems. Normal operations resumed nearly 10 days after the initial attack.

This incident revealed certain vulnerabilities in America's infrastructure. The heavily populated East and Southeast coasts have very few refineries and must rely upon a pipeline system to distribute its fuel needs. Furthermore, the latest cyberattack is confirmation of Abagnale's prescient warning from two years ago: Infrastructure is now a prime target for attack.

In the wake of the highly publicized Colonial hack, President Joe Biden issued an executive order to improve cybersecurity and create a blueprint for a more comprehensive federal government response to cyberattacks. Currently, and not uniformly, the FBI and Secret Service (due to the financial aspect of these crimes) are tasked with dealing with this increasing problem. A Ransomware Task Force recently issued a report to the Biden administration on how to combat this scourge. The report notes that companies hit by an attack took on average 287 days to fully recover.

The Colonial matter has once again cast a white hot spotlight on ransomware, in particular, and cybersecurity, in general. Ransomware has skyrocketed since 2012 when the advent of bitcoin and other cryptocurrencies made it difficult to track and ultimately block payments. And the work-from-home (WFH) phenomenon may have sparked a whole new economic subset fraught with potential problems.

Derek Thompson recently wrote a piece in The Atlantic magazine about WFH and the new hybrid work model. He uncovered an enormous technological shift that poses newfangled security challenges. The average worker invested 15 hours of time and $561 in home equipment to facilitate WFH in 2020. He adds, without a hint of hyperbole, that those figures are "an astonishing number -- amounting to close to 1 percent of annual GDP spent on WFH amenities." These figures don't even account for all the money companies spent on telecommunications, back-end systems, and other tech to support WFH. But are they protected?

The jury is still out. Unsurprisingly, however, as businesses shifted to remote work during the pandemic, it became apparent that many remote systems were not as secure as first thought. As a result, according to The Washington Post, 2,400 businesses, schools, hospitals, and government agencies were hit by ransomware in 2020 alone.

As Aretha Franklin sang in 1985, "Who's Zoomin' Who?"

KELLY FINANCIAL SERVICES LLC

On June 1, 2021, The New York Times realized the following: “Now, even small-time criminal syndicates and low-skilled hackers can pose a potential national security threat. Ransomware is easily obtained off the shelf, and virtually anyone can load it into a compromised computer system using YouTube tutorials or with the help of groups like Darkside. Customer support is included.”

Darkside was reportedly behind the Colonial Pipeline attack and is now believed to have shut down on its own accord. In the past, though, Darkside employed a technique known as “ransomware-as-a-service.” In this scenario it would partner with so-called affiliates who would actually conduct the attack. The affiliates would receive the lions share of the ransom proceeds. Even if Darkside has effectively disband, that should hardly give anyone comfort as bad actors will likely regroup and rename themselves. Cyber extortion has become more prevalent. And, notably, insurance policies covering ransomware became commonly available only about five or six years ago.

Cyber attacks are not new even if it appears they are getting more attention. In a plethora of statistics on its website that should give anyone the cyber bends, Purplesec, a cybersecurity company based in Vienna, Virginia, reveals this: In 2018, there were 80,000 cyberattacks per day (or 30 million annually).

More and more data reveal the financial damage done. According to Chainalysis, a blockchain analysis firm, ransomware gangs made at least $350 million in 2020, a 311% increase in payments recorded over 2019. The FBI received nearly 500,000 complaints of suspected cybercrimes in 2019, with reported losses exceeding $3.5 billion. And even more astounding, Cybersecurity Ventures predicted late last year that cybercrime would cost the world $6 trillion in 2021 (up from $3 trillion in 2015).

Last May, CBS News reported a “thriving” cybercrime environment and presented even more insights on the cost of these kinds of data breaches during the pandemic. The average cost of a data breach soared to $21,659, per incident, with most incidents ranging from as little as $800 to more than $650,000, based on information gathered in a recent Verizon report. And 5 percent of successful attacks cost businesses $1 million or more.

CNA Financial is one of those businesses.

Just days after Colonial was recovering from the attack on its operations, Bloomberg reported that CNA Financial, one of the country’s largest insurers, paid $40 million to hackers to regain control of its systems after it suffered a ransomware attack in March. (Yes, there is curious irony that certain attacks which garner more publicity may seemingly demand less direct ransom (notwithstanding indirect societal costs, like a spike in gas prices) while lesser known attacks may seemingly demand more ransom. But that is largely coincidental.)

Hackers actually do their homework and any discrepancy in ransom amounts is not, in reality, generally determined at random. Hackers are able to penetrate a given entity’s records -- such as email, and other entry points -- and may be able to roam undetected and unfettered for long periods of time. Accordingly, they effectively research the hacked target thereby allowing them to get a better sense of the target’s ability to pay.

KELLY FINANCIAL SERVICES LLC

Ransomware cyberattacks have clearly attracted much media attention of late. These attacks tend to be directed at the organizational level. Nevertheless, data breaches are a type of cyberattack that may have their greatest impact at the individual level.

The number of data breaches is just as alarming as ransomware incidents. In March 2021, statista.com reported that in 2020 the number of data breaches in the United States came in at a total of 1001 cases. “Meanwhile,” statista says, “over the course of the same year over 155.8 million individuals were affected by data exposures -- that is, accidental revelation of sensitive information due to less-than-adequate information security.” Remarkably, these figures represent a decline in number of cases and individuals affected reported in the years 2016 through 2019.

Still, the trends over the last fifteen years continue to be disturbing.

A sampling of the most notorious hacks during this timeframe is instructive for their breadth and depth of repercussions; they cut a wide swath of industry and sector. In every citation listed below (breach occurrence in parentheticals) at least one of three characteristics, if not more, were present: malicious attack, human error, system faults. Consider:

* TJX Companies [TJ Maxx, Marshalls] (Oct. 2007) - 94 million customers affected, MasterCards and VISA Cards compromised.

* Yahoo (late 2014) - 500 million users impacted. Several different large scale breaches of email, physical addresses, passwords, phone numbers, real names, dates-of-birth. Made public in September 2016.

* Ebay (May 2014) - 145 million users.

* Equifax (July 2017) - 143 million users. Included exposure of 209,000 consumer credit card details.

* Target (December 2013) - 41 million customers.

* Uber (late 2016) - 57 million users and 600,000 drivers. People outside the company accessed data on a third-party cloud-based service that Uber utilized; breach made public in Nov. 2017.

* Capital One (June - July 2019) - 100 million customers’ personal information compromised at one of the country’s largest banks. The breach included 140,000 stolen social security numbers and 80,000 bank account numbers, and tens of millions of credit card accounts. The hacker had formerly worked for Amazon Web Services (the cloud-hosting company), which hosted the bank’s database.

* Marriott International (starting in 2014) - 500 million guests’ data breached. The breach originally occurred on the support systems of Starwood Hotels. Marriott bought Starwood in 2016. Incredibly, perpetrators stayed in the network and were not discovered until Sept. 2018. Contact details, passport numbers, and travel details were among the information compromised. The breach was revealed in Nov. 2018.

* Facebook (supposedly fixed in August 2019) - Globally, 533 million Facebook users' data was exposed to the internet. The company allowed two apps to access its users' stored personal information on insecure servers without proper security measures.

* Massachusetts Registry of Motor Vehicles (March 2021) - A third-party vendor that facilitates vehicle inspections in Massachusetts (and other states) experienced a cyberattack across several states preventing vehicle inspections -- in Massachusetts, the system was knocked offline for nearly three weeks.

So, not only is our infrastructure vulnerable to attack, our retail outlets, our social media, and our financial institutions are vulnerable, too. A logical question to ask now: "What's next?"

Personal security and personal wealth.

Safeguarding oneself, family, property and money will likely become priorities given today's cyber risks -- especially given the sheer size of the financial assets at stake. In 2018, AARP reported that millennials are more susceptible to scams than seniors. But "those older than 50 are fleeced of more money overall." This makes sense. You may recall the gallows humor of Willie Sutton. When asked why he robbed banks, Sutton simply replied, "Because that's where the money is." From this emerged the Willie Sutton Rule. In the criminal sense this means: one's first choice should be to choose the most obvious route.

The obvious route today is a target-rich environment for cybercriminals. According to the Government Accountability Office (GAO), defined contribution retirement plans (such as 401(k) plans) held nearly $6.3 trillion in assets for 106 million enrolled participants in 2018. Last March, Voya Financial underscored the risk associated with these plans. It wrote that the GAO indicated retirement plans such as 401(k)s "face higher risk of cyberattack because the Labor Department has not clarified the cybersecurity responsibilities of employers and other fiduciaries or provided guidance for safeguarding employees' savings and personal data."

Out of the $28 trillion in U.S. retirement assets, some $5 trillion is in 401(k) plans, according to the Investment Company Institute, a mutual fund trade group. Given these staggering numbers, it stands to reason that if companies like Equifax, CNA Financial, and Capital One can be hacked, why wouldn't companies that are involved in defined contribution plans also be subjected to attack? Writing for forbes.com in 2018, John F. Wasik makes this important observation: "More worrisome for many plan sponsors [employers], the focus of cyberattacks in the defined contribution (401k) world has shifted from hardened targets like recordkeepers and custodians to plan sponsors, which often lack the extensive cybersecurity defenses of their vendors." Individual investors, therefore, need to ask pointed questions of their 401(k) administrators. In addition, Wasik implores, individuals need to know what kind of cybersecurity measures are protecting their retirement kitty.

Thieves will have even larger digital vaults to hack. Global assets-under-management are set to hit almost $150 trillion by 2025, Pensions & Investments reports.

Adopting a comprehensive personal security strategy is something individuals should seriously consider adopting. It is not as complicated as one may think. And there are a handful of high-

value steps in several areas where one's money, property, and personal information can be protected.

It is useful to return to Frank Abagnale for a moment.

He warned in the same interview with thinkadvisor.com, above, that "anybody can be scammed." Nonetheless, there are definitive signs that individuals should avail themselves of that portend scams. "No matter how sophisticated or amateurish," he counsels, in every scam there are two red flags: 1, the scammers say they need money immediately; 2, they ask for personal information (like social security number and date-of-birth).

In 2020, Fidelity Investments outlined in a white paper best practices in six areas that individuals can use to help themselves to thwart scams and cyberattacks. While no means comprehensive, the ideas conveyed below offer a starting point for self-awareness and self-protection.

-Make Yourself A Difficult Target for Cyber Criminals

-Understand and Protect Your Digital Footprint

-Protect Loved Ones from Elder Scams

-Keep Your Home Secure – People, Possessions, Information

-Properly Vet People with Access

-Travel Safely

1.) *Make Yourself a Difficult Target for Cybercriminals*

A. Protect Financial Accounts – Employ Extra Layer of Protection

- Two Factor Authentication (2FA)

- Strong and Unique Passwords

- Leverage Alerts on All Financial Accounts

B. Protect Your Email Accounts

- Don't Keep Sensitive Data (i.e., account numbers) in Email Folders

- Never Log Into Email or Financial Accts. from unsecure Wi-Fi Networks

- Be Aware of the Red Flags of malware/spyware/ransomware and phishing/pharming/smishing

C. Protect Your Mobile Acct.

- Manage "Trusted Device"

D. Protect Your Computer

- Anti-virus Software

- Keep Operating System up to Date

- Be Cautious with Email Attachments

2.) *Understand and Protect Your Digital Footprint* (Obvious = Facebook, Twitter, Instagram, TikTok, WhatsApp, LinkedIn; Less Obvious = Ancestry and Genealogy Sites, Professional Bios on Corporate Website, Real Estate Records – sales records, listings, video, photos)

- Be Aware of Your Total Household Exposure When it Comes to Sharing Personal Details on Social Media. Know What's Out There About You and Your Family

- Limit Disclosure (Don't Share Unnecessary Personal Details)

- Leverage Privacy Settings

- Don't Share Information as it Happens

- Periodically "Audit" Your Digital Footprint

3.) *Protect Loved One from Elder Scams* (One of the Fastest Growing Areas of Fraud is the Exploitation of Seniors and Those with Some Form of Diminished Capacity (i.e., dementia)

- Should be a Regular Topic of Conversation

- Create Oversight to Monitor Financial Accts. With at Least One or Two Trusted People

- Know Common Scams (engage AARP's "Fraud Watch Network")

- Set Up Automatic Alerts with Financial Institutions

- Remain Ever Vigilant (the World Health Organization estimates that 15.7 percent of people aged 60+ are subject to some form of abuse)

- If You Know of a Problem, Act Quickly – Alert Banks and Credit Bureaus (it is estimated that only 1 in 44 cases of financial abuse is ever reported)

4.) *Keep Your Home Secure – People, Possessions, Information*

- Have a Plan for Emergencies (medical, weather, fire)

- Don't Leave Personal Documents in Readily Accessible Place in Home (consider a digital repository for important documents – birth certificates, social security numbers, wills, trusts, financial statements, car titles, home titles, password lists)

- Secure Home Network (2FA, protect router, backup data)

- "Internet of Things" (coffee machines, thermostats, cameras, garages)

- Control Physical Access (track who has access to keys, alarm systems)

- Call for Help as Needed (police and emergency personnel)

5.) *Properly Vet People with Access* (Millions of Americans Employ Professional Service Providers with Household Access)

- Do Basic Research
- Don't Rely on 3rd Parties to Conduct Background Checks (do professional background checks)
- Consider Monitoring and Key Management (separate alarm codes for cleaners and contractors)

6.) *Travel Safely* (Often an Overlooked Area)

- Notify Banks and Credit Card Companies of Your Travel Plans (personal cards)
- Register with U.S. State Department Before Travelling Abroad
- Obtain Dedicated Travel Medical Insurance to Cover You Abroad
- Program Emergency Numbers in Your Phone (financial institutions, family, trusted friends)
- Receive all Recommended Vaccines
- Know Where to go in Case of Emergency
- Activate International Calling
- Avoid ATM Machines on Street Level (use inside bank/hotel)
- Backup Copies/Scans of Vital Documents (passport, travel itinerary, electronic ticket receipts)
- Stop Mail Delivery
- Don't Post Real Time Travel Plans on Social Media
- Protect Home While You're Away
- Take Necessary Medications with you in Original Containers in Carry-on Luggage

The COVID-19 pandemic saw a large increase in cybercrimes for corporations and individuals. Many people were working from home and certain security features on their equipment were lax -- as exquisitely revealed by hacked Zoom meetings, etc. And perhaps unsurprisingly, there were many scams surrounding pandemic relief as the government pumped trillions of dollars into the economy. It seems we are learning on a near-daily basis of schemers who defrauded massively funded efforts like increased unemployment benefits and the Paycheck Protection Program -- including devious plots concerning Covid vaccines, fake virus cures and charities. Fraud linked to the coronavirus cost Americans $382 million last year, disclosed the Federal Trade Commission.

As the pandemic fades from everyday life, it is important for individuals to remain vigilant about the threats posed by cybercrime. Such individuals may be well advised to talk with their financial advisors about the issue of cybersecurity, too. Starting that conversation may provide insights and actions to take to help protect individuals, their families, their property, and their money.

James P. Freeman is the director of marketing at Kelly Financial Services, LLC, based in in Greater Boston. This content is for informational purposes only and does not constitute an offer to sell or a solicitation of an offer to purchase any interest in any investment vehicles managed by Kelly Financial Services, LLC, its subsidiaries and affiliates. Kelly Financial Services, LLC does not accept any responsibility or liability arising from the use of this communication. No representation is being made that the information presented is accurate, current or complete, and such information is at all times subject to change without notice. The opinions expressed in this content and or any attachments are those of the author and not necessarily those of Kelly Financial Services, LLC. Kelly Financial Services, LLC does not provide legal, accounting or tax advice and each person should seek independent legal, accounting and tax advice regarding the matters discussed in this article.