Cyber Threats to Client Wealth & Well Being

Why & How Wealth Managers Will Soon Play a Key Role in Managing These Risks

March 2023

Mark P. Hurley

Carmine Cicalese

Bryce Washum

Douglas Garbutt

DIGITAL
PRIVACY &
PROTECTION

www.dpripro.com

Digital Privacy & Protection, LLC
Mark P. Hurley is the CEO of Digital Privacy & Protection, LLC. Carmine Cicalese is a Partner & Senior Adviser, Bryce Washum is a Senior Partner and Douglas Garbutt is Partner-in-Charge of Implementation.

Contents

Introduction

Warren Buffett describes cyber as "the number one" threat to mankind.[1] This is unremarkable given that cybercrime will soon be a $10.5T global business, represents the greatest transfer of wealth in history and is more profitable than the sale of all illegal drugs worldwide, combined.[2]

Cyber threatens financial assets, credit & healthcare, ability to earn a living & physical safety

Cyber risks now threaten every client's financial assets, their access to credit and healthcare, ability to earn a living and even physical safety. But most wealth managers currently do little to help manage them. This is surprising (if not stunning) given that:

- **Managing risks to wealth is already a core aspect of every firm's value proposition,**
- **Managing cyber risks would be both (relatively) easy and inexpensive,**
- **Doing so would also further cement client relationships,**
- **If (or more likely when) a client is hacked and/or has their identity stolen, it inevitably becomes the wealth manager's problem, involving potentially hundreds of hours of the firm's time, and**
- **Adding cyber risk management services provides a clear competitive advantage in marketing to prospective clients.**

Moreover, these risks are growing rapidly. Over the past two decades cybercrime has increased seventeen-fold, is up more than 600% since the onset of Covid and is expected to nearly double again over the next three years.[3] As microprocessors become more powerful and faster and the use of quantum computing expands over time, these trends will only accelerate.

Many firms have not come to grips with their own cybersecurity risks

Consequently, although most industry participants do not yet help clients manage cyber risks, this will change in the not-too-distant future. Granted, at first glance this may sound a bit farfetched and only a handful of wealth management firm executives will race to embrace the idea that they will have to do more work for clients for the same fees. In fact, many of them have yet to fully come to grips with their companies' own cybersecurity risks, much less consider how to manage those of their clients.

We also openly admit that we are biased. Our company provides a personal cyber protection service to families. The authors of this paper include a former senior military cyberwarfare officer and individuals who are experts in helping people protect both their cyberprivacy and cybersecurity.

---

[1] Business Insider
[2] Cybercrimemagazine
[3] Surfshark, CloudDB, Cybersecurity Ventures, Cybercrimemagazine

Regardless, for four reasons wealth managers soon will play a major role in managing client cyber risks:

(i) Doing so would be a natural extension of a core part of the value that they already provide,
(ii) Adding these services would be consistent with how their offerings have evolved over time,
(iii) If they want to remain as the trusted advisor to clients, at some point they will be forced into this role, and
(iv) It is in their material economic self-interest to address these risks upfront instead of after a client has been hacked and/or had their identity stolen.

Participants recognize they will have to help clients manage cyber risks

We also believe that most wealth managers already recognize that this will happen. Virtually every firm has had clients targeted for wire fraud and many have had to help those who were victims of identity theft.[4]

Additionally, as with every other major change to the industry over the past thirty years, wealth managers largely will approach the issue in two distinctly different ways. Most industry participants will take the "when it becomes inevitable, I'll do it" tactic, waiting until they are effectively forced to add cyber risk management services to their offerings.

However, another, smaller group of firms will capitalize on this coming change. They recognize that there are multiple surveys suggesting that prospective clients are quite concerned about these risks (but lack the knowledge and the means of easily and conveniently addressing them) and that their competitors are largely ignoring them.

An opportunity to distinguish offerings from competitors

Thus, instead of avoiding the issue, they will expand their offerings to address it and create a competitive advantage in their marketing efforts. It will allow them to distinguish themselves from that of their competitors by providing a more comprehensive service that addresses a broader range of risks to a client's wealth and well-being.

Three purposes of this paper

This paper has three purposes. First, it lays out why we believe that it is inevitable that wealth managers will soon play a significant role in helping clients manage cyber risks.

Second, it is intended to be educational and strip away much of the "mystery" that surrounds this topic. Anyone who has ventured into the cyber arena quickly learns that it has its own language and acronyms.

[4] The SEC has also endorsed the idea of advisers educating clients on these issues and has indicated that it views it as a measure of a firm's maturity.
https://www.sec.gov/investment/im-guidance-2015-02.pdf

Managing cyber risks is, quite candidly, not that complicated

And although they pose very real and serious threats to the wealth and safety of clients, managing them is, quite candidly, not that complicated.

Lastly, the paper is intended to provide a framework. One that wealth managers can use when thinking about how to structure their roles in helping to manage these risks.

Acknowledgements

The authors want to thank several people who were incredibly generous with their help. Two of the wealth management industry's most influential thought leaders are **Michael Kitces** and **Joel Bruckenstein.** Michael is the industry's top expert on practice management and his widely read online newsletter/blog regularly shapes the thinking of thousands of wealth management firm executives. Industry participants look to Joel for his advice on the newest and best technology and practice management tools. Both reviewed drafts, challenged our ideas and provided both criticisms and suggestions.

Allan Starkie is the Managing Partner of Knightsbridge Advisors, the top retained search firm in the wealth management industry. He has long been a thought leader on the future challenges that industry participants will face and has helped numerous firms recruit key executives, design their compensation systems, and identify their weaknesses and those of their competitors. Alan graciously spent a great deal of time serving as a sounding board for many of our ideas as well as reviewing this study and giving us his thoughts.

The terms iconic and wealth management are synonymous with two individuals: **Mark Tibergien** and **Harold Evensky.** Mark has advised and influenced almost every major wealth management firm at some point over his long and illustrious career. Harold literally wrote the original book on wealth management, was a key force in professionalization of the industry and built a very successful firm. As they have done with every other study that the authors have previously published, both provided us with many great insights, ideas and recommendations.

Tim Villano is the Chief Information Officer of Artemis Global Secure, one of the most sophisticated advisory/consulting firms to wealth managers, broker-dealers and private equity firms on information security issues. In addition to having a deep expertise in technology, Tim helps numerous wealth managers to understand and navigate the increasingly complex regulatory environment that they must now operate in with regards to cybersecurity issues. He very generously reviewed our drafts and provided several suggestions that are now incorporated into the study.

David Canter is the President of Bluespring Wealth Partners, LLC, which has provided capital to and partnered with twenty wealth management firms. Prior to Bluespring, he led Fidelity's RIA and Family Office segment and advised hundreds of industry participants on practice management, wealth management services, technology, and growth strategies. David reviewed drafts of the paper and was kind enough to share his thoughts and ideas on how to improve it.

Stuart Leaf is a successful entrepreneur who writes extensively. Along with co-author Daniel Doll-Steinberg, he will soon release a book on the immense impact of many frontier technologies, including many which already affect/control many aspects of our lives. Stuart reviewed multiple drafts of the paper and provided a series of insightful comments and suggestions.

The help provided by each of these individuals materially improved this study. However, its shortcomings are solely our own.

Mark P. Hurley

COL. Carmine Cicalese, US Army, Retired

Bryce Washum

Douglas Garbutt

For more information on DPP or our research, please contact us at info@digpp.com or visit our website at www.dpripro.com

I. Why Most Wealth Managers Will Soon Help Clients Manage Their Cyber Risks

The services provided by wealth management firms have continuously evolved over the past three decades. An industry in the early 1990s that was dominated by thousands of small companies that were largely asset allocators across mutual funds is today a collection of much bigger businesses that oversee most aspects of their clients' finances.

This evolution is far from finished and service offerings continue to expand to this day. Recent examples include investments in private equity, business and career advice and life planning to address the recent sudden increase in human life expectancy.

Cyber risk management will soon become integral to wealth management

However, we believe that there are four reasons that cyber risk management also soon will become integral to the services that wealth managers provide:

1. Risk management is a core part of the value already provided by wealth managers.

Managing various risks (i.e. investment, tax, estate, property & casualty and health care costs) to a client's wealth is a core part of the value already provided by wealth managers. Cyber creates three additional such risks as well as others that threaten a client's wellbeing:

A. Cybertheft

Clients are complacent about their financial liability

Nearly all financial assets are now digitized, and large sophisticated criminal cyber gangs are constantly trying to steal them. Many of these organizations operate openly in countries such as China, Russia, North Korea and Iran.

Unfortunately, far too many people have been lulled into complacency and have little idea of the financial risks they have when operating online. This is due in no small part to that two of their most widely used financial assets – i.e., credit cards and bank deposits – are protected by federal statutes and regulations. But, in virtually all other instances, they bear the preponderance of the risk of loss from cyber theft.

One example involves their custodial and brokerage accounts. Most of a client's liquid net worth is typically in assets held in these accounts.[5] In fact, many wealth management firms point to the independence of the custodians as a key source of comfort to clients that their assets are protected from theft.

At the discretion of the custodian to reimburse potential losses

However, the terms of use agreements to which the client is required to assent (but which they rarely read) generally are extraordinarily one-sided. They effectively make it at the discretion of the custodian or brokerage to reimburse any potential losses should the account be hacked. Similarly, the terms of use for virtually all online commerce sites require that their users indemnify the vendor – as opposed to the converse – should for any reason clients or the vendor suffer losses resulting from an online transaction.

B. Identity Theft

Only a small amount of information is needed for identity theft

A second key cyber risk that directly impacts a client's wealth is identity theft.[6] It requires only a relatively small amount of information—which is easy to obtain unless one carefully protects their cyber privacy – to steal someone's identity. Criminals use it to purloin credit, health insurance, government benefits and tax returns. There have even been instances of criminals assuming other parties' identities and posing as them when they are arrested. And their victims have been stunned to later learn that they now allegedly are convicted felons.

C. Reputational Risk

Online extortion and smearing are widespread

Clients' livelihoods are also directly threatened by cyber reputational risks. There have been thousands of instances of online extortion involving criminals who accessed embarrassing information on a device or in an online account without proper cyber privacy protections and who then threatened to publish it unless they were paid money. This crime is rarely reported because their victims often would rather pay the ransom than run the risk of being publicly humiliated and have their ability to earn a living irrevocably damaged.

---

[5] Assets in these accounts are not protected by federal statutes and regulations and are not insured by the FDIC. Brokerage accounts are insured by the SIPC up to $500,000 per account but only should the brokerage firm fail. However, the terms of use online agreements typically effectively require that the customer and not the brokerage bears the preponderance of the risk of loss from hacking.

[6] Protecting against identity theft is also now a critical issue for wealth managers themselves. They are required to develop and implement a written program that is appropriate to the size and complexity of the firm. And on July 27, 2022, the Securities and Exchange Commission ("SEC") separately charged three financial institutions with violations of Rule 201 of Regulation S-ID. require that the customer and not the brokerage bears the preponderance of the risk of loss from hacking.

Once a horrible allegation is on the Web, it is forever on the Web

Similarly, doxing[7] has been used to damage careers by taking information from unprotected online accounts and using it to create and publish online misleading half-truths. Many victims have been stunned to suddenly learn that that there are incredibly damaging false public allegations – such as that they were forced to leave a previous job because they sexually harassed someone or molested a child – being circulated online. Even more problematic, once such a horrible allegation is on the Web, it is forever on the Web.

D. Physical Safety

Criminals have adapted to technology & use online information to target victims

However, cyber creates risks that go far beyond just threatening clients' wealth. They also directly endanger their families' physical safety. Criminals have adapted to new technology and now capitalize on information from online accounts to target their victims. They use apps such as LinkedIn and Zillow to identify homes to burglarize and Google Street View to scout locations. And unless someone has carefully protected their digital privacy, it is uncomplicated for criminals to determine when someone is away from their homes and families.[8]

More troubling, nearly one third of all teenagers have already been stalked online by a "complete stranger."[9] Those families who do not carefully guard their cyber privacy make it easy for predators to gather a great deal of information about their children (and grandchildren). The information is often used – in a process known as "grooming" – by someone posing as a teenager who somehow "really understands" (and, thus, can emotionally connect with) one of their kids. Over time, the child is persuaded to trust the counterparty and share intimate information, including sometimes compromising photos.

In numerous instances, predators turn around and use this information to "sextort" the child into doing whatever they want. In one recent tragic incident, a 17-year-old boy who was an honor student committed suicide after such a predator began blackmailing him.[10] In fact, online "sextortion" has become so widespread that the FBI has created a separate unit to investigate such cases. Even worse, online stalking often evolves into physical stalking and there have been multiple instances of teenagers being tracked down and murdered.

---

[7] Doxing means searching for and publishing online with malicious intent private or identifying information about an individual.

[8] This often happens when an individual is on a trip and someone in their party posts a picture online. Unless the individual has engaged the numerous privacy settings and turned off both the "tagging" and facial recognition capabilities of certain apps, the photos and the names of the people included will automatically appear in third party accounts (including those of criminals), allowing them to see that the individual is away from his or her home.

[9] Brandon Gaille

[10] A 17-year-old boy died by suicide hours after being scammed. The FBI says it's part of a troubling increase in 'sextortion' cases. | CNN

Cybercrime Is Widespread

- More than half of all U.S. citizens have been victims of cybercrime.[11]
- One million passwords are stolen each week.[12]
- Nearly one third of Americans have had some portion of their identity stolen.[13]
- Two and a half million families have their health insurance stolen each year.[14]
- 43 million people have been "doxed."[15]

[11] Aite Group [12] SECplicity [13] Proofpoint [14] Identityforce [15] SafeHome

2. What family offices do today, wealth managers adopt over time.

It is not too difficult to predict the new services that wealth managers likely will add in the future. One need only look at what is being provided by family offices to their clients to see what is coming. To be sure, it is not as though wealth managers closely track what family offices are doing. However, there is a long track record of family office services eventually being adopted by wealth managers, albeit in a form that is useful for HNW clients.[16]

Most family offices manage client cyber risks

Today most family offices play a significant role in helping UHNW clients manage their cyber risks. This is due in no small part to that 28% of all family offices and their clients were targeted last year in cyberattacks.[17] Consequently, some have even recruited ex-FBI agents to oversee the family's cyber protection. Assuming the same decades-long pattern of services evolving from family offices down to wealth managers continues, then the issue is not whether wealth managers will at some point add cyber risk management services but rather how and when.

A few large wealth managers already provide such services

More importantly, this is already happening. A small number of very large (i.e., >$10B of AUM) firms now provide these services to certain clients. In other words, the adoption process has already begun and, thus, it is likely that it will be sooner rather than later that they will become widespread throughout the industry.

[16] We are defining high net worth (HNW) clients for the purposes of this paper as those with $3 million to $50 million of liquid investable assets and ultra-high net worth (UHNW) as those individuals with $50 million or more in liquid investable assets.
[17] RSM

3. When clients become victims of cybercrime, it quickly becomes their wealth manager's problem.

The third reason that we believe that wealth managers will likely soon provide cyber risk management services is due to a combination of client expectations and the headaches and costs involved when a client is hacked. More specifically, wealth manager client relationships have a resilience unmatched by any other industry. The stability is due in no small part to that clients view their wealth manager's role to be as much more than just providing financial advice. Rather, their wealth manager is their trusted advisor who they count on to help them solve their most important and urgent financially related problems.

Wealth managers have an unusual economic bargain with clients

Precisely because of this there exists an economically unusual bargain between most firms and their clients. Namely, the amount of work typically completed in the early months of a relationship is often much greater than that in later years. But the fees paid do not decline. Rather, they typically increase over time with market appreciation.

To be sure, the bargain has in part persisted because it takes clients an immense amount of time and energy to get set up and get their financial affairs in order. This, in turn, fuels a significant degree of inertia to the relationship. But it is also due to that many clients ascribe outsized value to having someone who they trust and can call when they need help in solving a complicated and important problem impacting their wealth.

Numerous surveys clearly show that cyber risks are already such a problem which concerns clients. However, most do not know what to do. And their inaction has significantly increased their likelihood of at some point having a very adverse online event.

Understandable that clients expect wealth managers to help when they are hacked

This is problematic for industry participants because clients often believe that it is their wealth manager's job to help them when they are hacked and/or have their identity stolen. This is particularly understandable given that both are direct threats to their wealth.

Certainly, some firms have tried to tell their clients that helping address these issues is not part of what they do. However, several executives who we interviewed found that doing so often perplexed and upset clients. Moreover, the executives invariably decided that it was far preferrable to help the client instead of potentially endangering their role as the client's trusted advisor and forcing a closer examination of the ongoing value provided versus the fees paid.

Multiple surveys show that individuals are concerned about cyber risks

- 91% of Americans are worried about online security threats[18]
- 63% are worried that their identity will be stolen[19]
- 81% are concerned that their connected devices pose a threat to their privacy.[20]
- 79% are concerned about the online data that is being collected about them[21]
- 72% of respondents are very or extremely concerned about their online privacy[22]
- 73% of consumers would reconsider using a company if it failed to keep their data safe[23]
- 61% believe their household could be the target of an attack in the next year[24]

However, most have not yet taken the necessary steps to protect themselves

- 90% of Internet users do not know how to protect themselves online[25]
- Nearly two thirds rely on memory instead of a password manager[26]
- One third are more concerned about being able to remember a password than to have it secure[27]
- Only 16% take the necessary steps to protect their cyberprivacy[28]
- 61% of those who have taken steps to protect their digital privacy are under 45[29]

[18] Sophos [19] Norton [20] Chubb [21] Pew [22] Startpage [23] Deloitte [24] Sophos [25] Mozilla
[26] Business Insider [27] Bitwirden [28] Ipsos [29] Cisco Consumer Privicy Survey

4. It is in the wealth manager's material economic self-interest to help manage cyber risks upfront.

The worst point to begin managing cyber risks is after a client is hacked

However, the worst possible point at which to begin helping clients with cyber risk management is after they have been hacked. Depending on what has been stolen, repairing the damage could involve hundreds of hours of unpaid work by the wealth manager involving the FTC, law enforcement and passport agencies, credit card companies, vendors, and credit bureaus.

Even worse, fixing these problems also typically takes a lot of the client's time and money. In the interim, they can become very frustrated and unhappy.

Repairing damage could involve hundreds of hours of unpaid work

The only alternative to avoid this quandary is for wealth managers to instead proactively help clients to protect their digital privacy and security on the front end. Then such bad events become far less frequent. More importantly, when they do occur, the resulting damage usually is much smaller and fixing it takes a lot less time and money.

Additionally, (and somewhat ironically), a byproduct of playing a robust role in helping manage client cyber risks upfront is that it further cements the wealth manager / client relationship. These threats are continuously evolving and helping address them provides industry participants another means of regularly demonstrating value. And as will be described in detail in the latter chapters of this paper, after the client completes the associated set up process and becomes accustomed to using certain technologies, replacing one's advisor becomes a much more burdensome and aggravating task.

II. How HNW Clients Are Likely to Be Targeted by Cybercriminals

The first step in managing cyber risks is to understand how clients are likely to be targeted. It is important to keep in mind that HNW clients are viewed differently by cybercriminals than UHNW clients. The latter are effectively financial institutions from which there is an opportunity to steal large amounts of money. Consequently, criminals often will be willing invest a lot of time and resources to see if they can get around an individual UHNW client's cyber defenses.

In contrast, successfully attacking HNW clients is typically far less lucrative. They have much fewer, easily transferrable liquid assets than do UHNW clients and generally their assets are held in bank, brokerage and custodial accounts that have multiple layers of cyber protections. Thus, even if the hackers are successful, it would require about the same amount of effort to steal from a HNW client as it would from a UHNW client, but the reward for doing so would be far less.

HNW clients are most often targeted through mass attacks

Consequently, HNW clients are most often targeted through mass attacks – i.e., those involving thousands of people and their accounts at once. That much said, cybercriminals will not hesitate to go after HNW clients directly if they (i) do not carefully protect their cyber privacy; (ii) make it easy to breach them; and/or (iii) suspect that clients use their personal devices and accounts for work.

A. Mass attacks

Mass attacks typically take one of two forms:

(i) Direct attacks.

Direct attacks are computer-driven attempts to guess passwords

Cybercriminals use computers in direct attacks to try and guess passwords for tens of thousands of accounts at once. They often take passwords compromised in corporate data breaches along with unprotected online information about individuals and, with the help of sophisticated algorithms, generate thousands of variations of each password. The hackers then take these passwords and the client's email address and try to breach their other online accounts.

Clearly, if someone uses the same or similar passwords for multiple accounts, almost of them will quickly be compromised. Likewise, direct attacks are often successful when passwords include personal information (i.e., children's, friends' or pet's names, their alma mater or nickname, etc.), and/or are relatively short and lack special characters.

(ii) Malware.

Another common way in which HNW clients are targeted is through phishing[30] emails and smishing[31] texts with links that, if clicked on, download malware onto a device. Malware takes many forms and is designed to capitalize on gaps in device operating systems. Some versions automatically export data from the device. Other ones track the keystrokes of the user to learn the passwords being used.

Malware is software that gets around cyber defenses

Although anti-virus software detects and blocks most malware, criminals are constantly innovating new versions of it. Hence, it typically can – at least temporarily – get around these defenses, especially when operating system software is not regularly updated for the latest patches and anti-virus software is not kept current.

Phishing emails and smishing texts carrying malware often look very realistic and appear to have been sent by legitimate parties. And although almost everyone has been told to never open them – much less click on the link – worldwide this happens more than one billion times per day.[32]

Criminals also create fake apps (known as "Trojans") that, if clicked on, download malware onto a device. Trojans mimic the appearance of other apps and promise features that are potentially very appealing. Many are also created specifically for children.

B. Capitalizing on poor cyber privacy

As described earlier, cybercriminals largely target HNW clients through mass attacks. However, if someone is careless in how they operate online, the bad guys will not hesitate to go after them directly.

Easiest targets are those who don't protect their cyber privacy

From the perspective of cybercriminals, the easiest target is someone who fails to protect their cyber privacy. More specifically, unless one limits the personal information that they place online and carefully controls who can access it, a criminal does not have to hack an account to obtain large amounts of personal information about a target. Rather, it is simply out there for the taking and can be used to steal their identity.

Notwithstanding this, many individuals fail to engage the necessary privacy settings on their online accounts, control which information may be shared with others and/or who can access it.

---

[30] "Phishing" is an attempt to acquire sensitive data through a fraudulent email solicitation in which the perpetrator masquerades as a legitimate business or reputable person.
[31] "Smishing" is the fraudulent practice of sending text messages purporting to be from reputable companies.
[32] digitalintheround, www.cybertalk.org

Some make it easy to steal their identity

Some even include their (actual) birth date, biography, photos and other personal information on various sites. It is as though they are trying to make it easy for someone to steal their identity.

Far more problematic, this same information is often used to target children (and grandchildren). Unless parents and grandparents are vigilant about guarding their families' cyber privacy, predators can quickly figure out where children live, go to school, their extra-curricular organizations and their friends.

C. HNW clients often make it easy for criminals to breach their devices

Cybercriminals also will directly target HNW individuals who make it easy to breach their devices in the following ways:

Criminals use public WI-FI to copy passwords

(i) Using Public WI-FI without a virtual private network (VPN)

There is a reason that, when connecting to most public WI-FI sites, users are required to acknowledge that they are not secure – it is because criminals using the same WI-FI site can see what others are doing on their devices. In what is referred to as an "over-the-shoulder" attack, thieves will often spend hours each day at a coffee shop or a hotel with free public WI-FI copying passwords whenever other users input them into online sites. Sometimes the criminals will even create fake free public WI-FI sites using a hotspot that make it even easier for them to watch others operating online.

This form of hacking is impossible to detect but is preventable if one uses a virtual private network (VPN). VPNs are software that encrypts a user's online traffic and prevents third parties from viewing confidential information such as passwords.

(ii) Leaving devices (even briefly) unattended

It takes a criminal only seconds to download a Trojan onto an unattended device.[33] Such occurrences are common at expensive resorts as well as when one is overseas. In fact, many Fortune 50 companies are so concerned about this risk that they require board members to use burner phones whenever they are out of the country.

[33] It is important to note that the criminals are not trying to steal the device but, rather, in just seconds they can install a Trojan/malware. In fact, they want the owner to continue to use it because the malware will enable them to capture their passwords and other confidential information.

Public charging stations download information & upload malware

(iii) Using public charging stations or rental cars without a USB blocker

HNW clients also make it easy for hackers by using either public charging stations (such as at airports) or by plugging their phone into a rental car and, in either instance, not using a USB blocking device. The charging stations are typically assembled in countries such as China and often download a device's information while at the same time inserting malware. And when clients connect their devices to rental cars (usually to charge them and/or use the device's GPS), the vehicles often download the connected device's data. More than a few enterprising workers at many rental car companies often enhance their income by downloading this information from returned vehicles and selling it.[34]

USB blocking devices are prophylactic tools. They allow devices to charge while at the same time block the download of data and/or insertion of any malware into the device.[35]

(iv) Leaving Bluetooth on when not using it

Bluetooth technology is a great invention that makes it much easier to access devices. Unfortunately, it also allows others who are physically proximate to access the same devices. And given that the default setting on most devices for Bluetooth is on, a third party can anonymously access a device that is being used by its owner.

Consequently, hackers – in public places like airports, coffee shops, hotels – will access other people's devices by connecting to them through Bluetooth and copy the information that they find on them. There have even been instances of company executives on flights having their laptops hacked by someone using Bluetooth sitting four or five rows behind them.[36]

Smart home technology is by far the easiest to hack

(v) Smart Home Technology.

However, by far the easiest way for hackers to breach a HNW client is through smart home technology. Cybercriminals look for homes with security cameras, digital lightbulbs and smart door locks. This kind of technology is relatively easy to hack, and one need only breach a single piece to compromise every device connected to the entire home network.

[34] CNN
[35] Some examples USB Blockers include PortaPow USB data blocker, USB Data Blocker, JSAUX, and Offgrid USB data blocker.
[36] securityledger.com, Zee Business, The Street, fcmtravel.com.

Unfortunately, clients often make it even simpler for criminals to do so. For example, many use the default password settings on their home smart technology devices instead of creating unique and complicated passwords. Others throw away smart lightbulbs without removing the attached microchip.[37] Criminals regularly rummage through trash looking for them because the chips contain the password necessary to breach the entire home system.

D. Use personal devices and emails for work

Although cyberthieves generally will not spend a great deal of time and resources to try and hack a HNW individual, they often will make an exception to this rule if they believe that doing so will allow them to access work information. Most companies have explicit policies about not using one's personal devices and email accounts for work matters. However, not everyone strictly adheres to these rules and cybercriminals look to take advantage of this.

Easy to identify & target executives and owners of companies

The bad guys typically seek two types of opportunities. The first is to find valuable confidential information (company financial statements, trade secrets, etc.) It is not difficult to identify the executives and owners of companies and, as noted earlier, it is far simpler to hack them at home than at work. And given the potential value of confidential information, hackers will often invest a great deal of time and resources to go after such targets.

The second type of criminal opportunity involves finding information on personal devices which hackers can use to breach an employer. Even though a company may have robust cyber security protections, it does not take much for an employee to inadvertently create such an opportunity.

Thieves steal work information from personal devices & email accounts

For example, many companies require that employees use a password manager for all work matters. However, should an employee access their work password manager using a personal device, that device's Web browser will often automatically capture and record online account information and passwords from the password manager. And if a hacker can breach the device, this work information is now easily accessible.

[37] Hackster.io

III. It Is Not Complicated to Protect HNW Clients From the Overwhelming Majority of Cyber Risks

Basic cyber hygiene protects against overwhelming majority of cyber risks

Although cyber threats pose very serious risks to HNW clients and their families, it is relatively uncomplicated for wealth managers to help protect them. More specifically, there are a series of simple steps that clients could and should take on their own (but often do not) that will significantly reduce their exposure. Collectively they are referred to as operating online with "basic cyber hygiene."

To be sure, the first rule in cybersecurity is that one must accept upfront that everyone will be hacked and/or have their identity stolen at some point, regardless of what they do. The only issues are how frequently this will occur and how much damage will accompany it.

Everyone gets hacked – only issues are how frequently and the resulting damage

Why? Criminal cybergangs have immense resources and processing power and are often backed by nation states such as Russia, China, North Korea and Iran. They also include military cyberwarfare officers who by day are engaged in attacking Western countries and, by night, moonlight stealing assets online. They have demonstrated repeatedly that they eventually can breach anything that they target including companies, cloud services, blockchain and even national security agencies such as the DOD and CIA.

Hence, operating online with basic cyber hygiene does not eliminate cyber risk. Rather, it reduces and helps manage it by making one a more hardened – and therefore, a less attractive – target and by being prepared to identify any breaches and quickly take the necessary steps to repair them to minimize the resulting damage. It also effectively compartmentalizes one's information and thus, limits what criminals can access from a single breach.

Bears and Cybersecurity

An easy way to help clients think about how to protect themselves and their families from cyber risks involves an old joke about two guys walking through the woods who stumble onto a bear. They take off being chased by the bear, but one suddenly stops and puts on a pair of track shoes. The other person points out to him that, even with track shoes, no one can outrun a bear. The first replies "I don't have to outrun the bear. I just have to outrun you."

Similarly, when it comes to cyber, no one can completely prevent the possibility of being hacked. However, if one makes themselves a harder, less attractive target, the cyber criminals will often just go after someone else.

Basic cyber hygiene can be broken into two general categories: creating a layered digital security structure and ongoing risk management.

A. Technology for a layered digital security structure

Creating a layered digital security structure requires a combination of technology and numerous steps.

There are four types of technology needed:

Four types of technology are needed for a layered digital security structure

(i) Virtual private network (VPN)[38]

As described earlier, a VPN is software that encrypts one's online traffic. It both prevents others from seeing what one is doing on a device and prevents websites from identifying and tracking the person using one.

(ii) Password manager[39]

A password manager is encrypted software that stores an individual's passwords for each of their online accounts.

(iii) Private email[40]

A private email (unlike Outlook, Gmail, AOL, etc.) is not automatically read and mined for data. It does not replace one's existing, daily-use emails. Rather, it provides materially greater cybersecurity when used for double authentication purposes (vs. using text messages to a smart phone) for online accounts involving material amounts of money and social media accounts with large amounts of personal information.[40] It also is often used for sensitive emails (i.e., communications with counsel or a physician, very personal matters, etc.) with content that one would not want to have automatically read and potentially disseminated.

(iv) Up-to-date anti-virus software

Anti-virus software is the first line of defense against malware and most people have some form of it on their devices. However, if it is not regularly updated, it becomes ineffective.

[38] There are dozens of VPN providers. Some of the larger ones include Express VPN (www.expressvpn.com), Surfshark (www.surfshark.com), NordVPN (www.NordVPN.com) and ProtonVPN (www.protonvpn.com)

[39] There are likewise dozens of password manager providers. Some of the larger ones include Keeper (www.keepersecurity.com), LastPass (www.LastPass.com) 1Password (www.1Password.com) Dashlane (www.dashlane.com) and Bitwarden (www.bitwarden.com).

[40] There, too, are many private email providers. The larger ones include OpenSRS (www.OpenSRS.com), Titan (www.titan.email.com), Protonmail (www.proton.me), Tutanota (www.tutanota.com) and Mailfence (www.mailfence.com).

[41] Using a private email provides significantly better cyber security than mobile phones when double authenticating online accounts because cell phones are very easy to "spoof"(i.e., copy their SIM cards while walking by their user) allowing a criminal to "jack" or remotely takeover the device. In contrast, private emails can be set up with their own double authentication, creating a further layer of protection when authenticating online accounts involving sensitive personal information or potentially large amounts of money.

Cybersecurity Technology Diligence

There are numerous providers of cyber protection technologies, and many do a great job of protecting information. However, it is important to carefully diligence them because several are not user-friendly and can make it much more complicated and slower for clients to operate on the Web.

Additionally, it is essential to diligence whether the providers of technology use them to collect information on their users. This is commonplace with companies backed by Iran, Russia and China as well as with those technologies that are offered for free or as a no-charge-add-on to an existing service (e.g., a cable or an identity protection company offering a free VPN or password manager). But there are also several paid providers who collect and sell user information but rarely disclose this upfront.[42]

Lastly, it is important to select technology that has been independently vetted by sophisticated third parties. Unfortunately, many of the technology "ratings services" are sponsored or even owned by providers. And invariably the provider's technology is ranked in their reports as one of the "best."

[42] This information often only shows up in an obscure section of the supplemental agreements for their services.

B. Creating the layered digital security structure

There are seven steps required to create a layered digital security structure:

Seven steps to creating a layered digital security structure

(i) Install a VPN, password manager and private email on each device.

Each of these technologies should be installed on every smart phone, laptop and desktop computer and tablet used and the client should be taught how to use them.

(ii) Populate password manager with online accounts and resetting their passwords.

Every online account that a client has should be added to their password manager and their passwords should be reset using unique, randomly generated 15 to 20 alphanumeric character passwords.

Hundreds of privacy & security settings need to be engaged

(iii) Engage privacy settings on online accounts.

As noted earlier, many online accounts allow users to effectively opt out of their data collection efforts as well as limit who else can access their information. However, because collecting and selling user information is a core business activity of many online companies, correctly doing this will often involve navigating a maze of different web pages to engage the necessary dozens of settings for each account.

Private email is a more secure way to double authenticate important online accounts

(iv) Engage double authentication settings on online accounts.
Many online accounts have an additional layer of security which, if engaged, requires a user to provide two forms of authentication to log in. Although some sites require that a mobile device be used when providing a second form of authentication, as described earlier, it is preferrable whenever possible to instead use a private email.

(v) Engage privacy and security settings on devices.
There are also numerous privacy and security settings that should be engaged on each device. It is important to engage the capability to wipe a device remotely should it be lost and to turn on the necessary settings to prevent apps on the device from gathering and selling the client's information. Additionally, it is likewise essential to engage the necessary settings to prevent third party software from automatically copying and storing passwords and to prevent apps from turning on the device's microphone and camera without the user's permission.

(vi) Engage the privacy and security settings on Web browsers and search engines.
While one is engaging the privacy and security settings on devices, it is important to also engage the privacy settings on Web browsers and search engines. Absent such settings, browsers and search engines will both track a user's online activity and gather large amounts of personal information that will be sold to third parties.

(vii) Ensure each device has up-to-date anti-virus software.
At some point all devices become infected with malware. Ensuring that each device has current anti-virus software is analogous to keeping one's vaccinations current.

C. Ongoing risk management

There are six critical elements to managing risk after one has created a layered digital security structure:

Six steps for managing ongoing cyber risk

(i) Monitoring the Dark Web and corporate data breaches.[43]
Given that it is inevitable that everyone will at some point be breached and/or have their identity stolen, a critical aspect of cyber risk management is being able to detect when this occurs. The Dark Web is a segment of the Internet used by criminals and terrorists and is where stolen information is typically sold. There are numerous services which individuals can subscribe to that allow them to track whether any of their information has been stolen and is being offered for sale.

(ii) Retrieving and reviewing credit reports for the entire family annually.
Each of the three largest credit monitoring bureaus annually will provide free copies of credit reports. These reports are analogous to a blood test for identity theft because abnormalities that appear on them often indicate that one's identity has been stolen.

It is also important to check annually to see if there are credit reports for one's underage children. Understandably, if one exists it often means that another party has assumed their identity.

Early detection of breaches or identity theft reduces the resulting damage

(iii) Being prepared to quickly address stolen information or identity theft.
As noted previously, the best way to minimize the damage from either a breach or stolen identity is to detect it as early as possible and to quickly take steps to address it. This may be as simple as changing a single password or as complicated as having to make filings with multiple parties and, in certain circumstances, freezing or limiting credit and transferring assets to new accounts.

(iv) Wiping lost and retired equipment.
Another core aspect of operating with basic cyber hygiene is wiping any information that is stored on lost and retired devices. Provided one has engaged the necessary settings and the lost device is connected online, wiping it is uncomplicated.

[43] Some such services include: IdentifyForce (www.identityforce.com); identityguard (www.identityguard.com) and ID watchdog (www.IdWatchdog.com). However, while they provide Dark Web monitoring, their other services are at best ineffective cyber protection when compared to having a layered digital security structure with ongoing risk management.

Retired devices include anything no longer being used that has collected and saved client information such as computers, smart phones, tablets, home assistants and leased autos.

(v) Educating the client's entire family about cyber risks.
No different than any other risk management program, education plays a key role in managing cyber risk. And as noted earlier, a single misstep (clicking on a link, leaving a device unattended, etc.) can compromise a digital security structure.

Both clients and their children need to be educated about cyber risks

Consequently, both clients and their children need to be educated about risks and how to operate online with basic cyber hygiene. And given that there is no limit to the creativity of cybercriminals, education programs must be ongoing and include new threats and risks.

(vi) Process of regularly updating protection.
Online accounts regularly change privacy and security settings. Clients also get new devices over time. They also stop using certain online accounts and apps and add new ones. And eventually, they make mistakes.

Unless all aspects are current, a structure quickly becomes ineffective

More importantly, unless all aspects of a cyber structure are kept current, the entire structure quickly becomes ineffective. Consequently, operating online with basic cyber hygiene requires a regular updating process.

(vii) Reviewing one's digital footprint at least annually.
An essential aspect to figuring out exactly what needs to be updated is to conduct a comprehensive review at least annually of one's digital footprint. Integral to this process is looking for various symptoms that devices or accounts may have been breached and then taking the necessary steps to address any resulting concerns.

IV. A Framework for Helping Manage Client Cyber Risks

We (as well as numerous public surveys) have found that most clients already recognize and accept that how they currently operate online is unsafe. Moreover (and as described earlier), clients could and should on their own already take the steps necessary to protect themselves and their families.

They are not complicated. However, they can be very time consuming. They involve identifying hundreds of online accounts, installing them in a password manager, resetting their passwords, and then engaging hundreds of privacy and security settings for online accounts, browsers, devices and search engines.[44] For many clients, just thinking about the work and time involved is exhausting.

Challenge: Get clients to do something they know they should do but won't do

Consequently, most clients choose to not do anything until after they have suffered a very adverse event. And this quickly becomes problematic for industry participants because clients then expect that it is their wealth manager's job to help fix it, potentially consuming countless hours of the adviser's time.

In other words, wealth managers face a vexing dilemma. For their own economic self-interest, they need find a way to get clients to do something that the clients already accept that they should do but still refuse to do. It also would be most ideal if they could get clients to pay for everything involved and if the process of doing so further attached the client to the wealth manager.[45]

Accomplishing this requires six elements:

Economic model is based on providing high intellectual capital services

1. Proper definition of the wealth manager's role.

The first is to properly define the wealth manager's role. More specifically, firms in this industry generally are not good at high volume, low margin activities. Their economic model is based on providing scalable high intellectual capital services and they typically outsource (and have the client separately pay for) processing functions.

For example, most wealth managers do not prepare tax returns. But they do provide tax advice. The former is a processing function for which the client retains an accountant.

---

[44] There are nearly 300 privacy settings that should be engaged for just fifteen of the most-commonly-used apps. Figuring them out – as well as those for other apps – can take dozens of hours. And every year they must be updated.

[45] As noted earlier, all of this is conditioned on that a wealth manager already has taken the necessary steps to deal with its own cyber risks. According to the SEC, nearly three quarters of all industry participants have been targeted in cyber-attacks. However, large number of firms are still only just beginning to address these issues.

The wealth manager then reviews the returns to identify opportunities for the client to be more tax efficient.

Most wealth managers will partner with vendors

Hence, we believe that most wealth managers will partner with outside providers to help clients manage their cyber risks. More specifically, they will rely on vendors to:

- To help get clients digitally organized,
- Evaluate, set up, and install technology,
- Engage hundreds of privacy and security settings, and
- Regularly update everything.

Additionally, if (or more likely when) a client has assets and/or their identity stolen, they likewise will turn to a third party to assist the client with the necessary work involving fixing it. The wealth manager will oversee these processes and their providers. And as always, the adviser will serve as the client's advocate and ensure that any problems are fully addressed.[46]

2. Provides protection appropriate to the likely threat.

Doing more than basic cyber hygiene adds little

As noted earlier, likely online threats are tied to the size of a client. While UHNW clients need cyber protections comparable to financial institutions, for HNW clients the overwhelming majority of cyber threats can be addressed by helping them to operate online with basic cyber hygiene. Doing much more than that generally significantly increases cost and complexity without materially improving a client's protection.

3. Is relatively inexpensive for clients.

Although clients are very concerned about cyber risks, they typically are only willing to pay for services that, from their perspective, are relatively inexpensive. More specifically, for billionaires paying $7,500 to $10,000 per year to protect their cyber privacy and security is a de minimis expense. Not so with HNW clients.

Cost must be much less than $1,000 per year

In our experience, the typical HNW client would view as little as $1,000 per year as being exorbitant. And unless the cost is significantly less, either the wealth manager will have to pick up the tab or clients would rather take their chances continuing to operate online in the same manner as they do today.

[46] There are some very successful industry participants that prefer to personally deliver every service provided to their clients, even if doing so may not be profitable, much less economically optimal. Some may elect to create specialized units within their companies that provide these necessary cyber protection services.

4. Has a set up process that is painless for clients.

As important as price is, an even bigger barrier to getting clients to take the necessary steps to protect themselves is the time and work involved. Hence, it is essential that any cyber protection services provided allow clients to get quickly and painlessly digitally organized.

Digital organization process must take three hours or less

In our experience, unless the organizational process can be completed in about three hours or less, most clients will just give up. However, it can be quite challenging to make this happen.
It requires teams of experts working simultaneously on each of the client's devices. And at the same time there must be an oversight system to ensure that no client information can be misappropriated in the process.

5. Incorporates technology that is easy to use and is supported.

Technology has to have 24/7 support

Equally important to a satisfactory client experience is that the technology provided be easy for an average person to use. Otherwise, clients will quickly become frustrated and angry. Additionally, as with all technology, there are times when it will not work perfectly. Thus, the services must include experts ready and available to help clients, day or night.

6. And involves a B-2-B-2-C relationship with vendors.

Once digitally organized & accustomed to using technology, change is unappealing

Once a client is digitally organized and then he or she becomes accustomed to using specific technologies to operate safely online, it creates a degree of inertia. More specifically, it quickly becomes very unappealing to most clients to have to redo the organizational process and change their cyber protection technology.

Wealth managers can capitalize on the inertia and use it to further cement their client relationships if they properly structure their agreements with vendors. Integral to this is having a B-2-B-2-C relationship.

More specifically, it is essential to the wealth manager's protection from potential liability that the client's agreement is with the vendor. However, it should include a termination clause that is triggered if the client elects to fire the wealth manager.

Aspects of cyber protection services to avoid.

While it is essential to include these six elements when structuring the process for managing client cyber risks, at the same time there are four other aspects of potential cyber protection services that wealth managers should avoid:

1. Proprietary technology.

Proprietary technology requires immense amounts of ongoing CAPEX

Cyber protection services which offer "proprietary" technology can be potentially very problematic. While including it in an offering may sound great, it typically significantly increases cost, often makes it much harder for the client to operate online and – worst of all – only rarely materially improves protection for HNW clients. Moreover, its provider must have the capital to continually reinvest in maintaining and improving the technology or it will quickly become obsolete.

In contrast, there are numerous off-the-shelf technologies that are widely used, provide substantial protection and have been independently vetted by multiple third parties. Additionally, the off-the-shelf technologies are specifically designed to be easy for consumers to use.

2. "Swatting a fly with a sledgehammer" services.

Company-level and UHNW client protection services are overkill for HNW clients

Some cyber protection services include impressive sounding attributes such as "company-level technology" or services such as "custom firewalls" and "penetration testing." While many may make sense for certain companies and UHNW clients, they are largely overkill for most HNW clients given how they are likely to be attacked. Consequently, they usually do not materially improve a client's protection while at the same time increasing cost and making it much more cumbersome for the client to operate online.

3. "Feel good" cyber services.

Many cyber protection services sound beneficial but do very little

There are also a host of cyber protection services that perhaps sound very beneficial but do very little to help protect clients. Two such examples are companies that offer to conduct "cyber intelligence" analyses and others that provide services to clients to opt out public databases.

Cyber intelligence analyses are designed to help companies identify which parties are likely targeting them to help them to better adjust their cyber defenses to address these threats. However, as noted earlier, it is insufficiently lucrative for criminals to invest a lot of time and resources in directly targeting HNW families unless they make it very easy to come after them. Thus, although including this type of analysis as part of a service may sound impressive to a client, they usually are of little value.

Similarly, several cyber protection companies include services which help clients to opt out of databases. Hundreds of companies maintain large scale databases with immense amounts of information on individuals, gathered from public and private sources and that is sold to third parties. Under the law, one has the right to opt out of a database and any information associated about him or her at that point in time in the database must be deleted. And because making the necessary filings can be a very time-consuming process, several companies offer to do this for a fee.

Opt-out of database services are analogous to Whack-a-Mole

Unfortunately, the opt out process is generally a pointless exercise. Most data companies have many different databases, and the law allows them to transfer information from one to the other almost immediately after it has been deleted from the first one. Thus, the opt-out process quickly becomes analogous to a game of "Whack-a-Mole".

Additionally, it is not difficult for data companies to replace any deleted information because state and municipal governments regularly sell it to them. In fact, the sale of such information has become a key source of revenue for many states and cities.

4. Personal cyber insurance.

Wealth managers should be cautious about considering cyber protection services for their clients which include personal cyber insurance. To be sure, it is appropriate for (and is widely used by) companies to mitigate the potential costs of fixing a major data breach or a ransomware attack. Last year alone there were $4.9 billion in premiums paid on such cyber protection policies.[42]

Very challenging to collect on the guarantees/insurance provided by many online identity protection services

However, the cyber insurance market for families is often very different than that for companies. For example, several online cyber protection companies market their services by providing either insurance or "guarantees" to reimburse up to $1 million of costs should a client be hacked or have their identity stolen. Unfortunately, the terms of the insurance or guarantees often make collecting on these policies potentially very challenging.

For example, their terms often include an out for the insurer if the client's "negligence" played any role in causing a breach or identity theft. This is an extremely low legal threshold and makes it easy for insurers to dodge any liability. Additionally, the insurance and guarantees are often structured as umbrella policies – i.e., the client must first sue everyone else involved, collect what he or she can and only then can try to collect the difference from the insurer. The costs of this additional layer of litigation are potentially much greater than any amounts that the client might ultimately recover from the insurer.

[47] NAIC

Many policies likewise make it difficult for clients to get the qualified professional help to fix breaches or identity theft because they cap what the insurer will reimburse for either attorneys (as little as $125 per hour) or accountants (only $80 per hour).

Lastly, several policies require that the client agree to binding arbitration and, in certain cases, should the client lose, he or she would be obligated to reimburse the insurance company's fees and costs.

Relative tradeoffs of cost & benefit from various potential cyber protection alternatives

On the accompanying page, we have graphed out what we believe is the relative cost/benefit tradeoff from various cyber protection alternatives. Those items above the line are critical to helping clients manage their cyber risks. However, those below the line often are very costly, make it significantly harder for someone to operate online and provide very little marginal improvement in cyber protection for a HNW client.

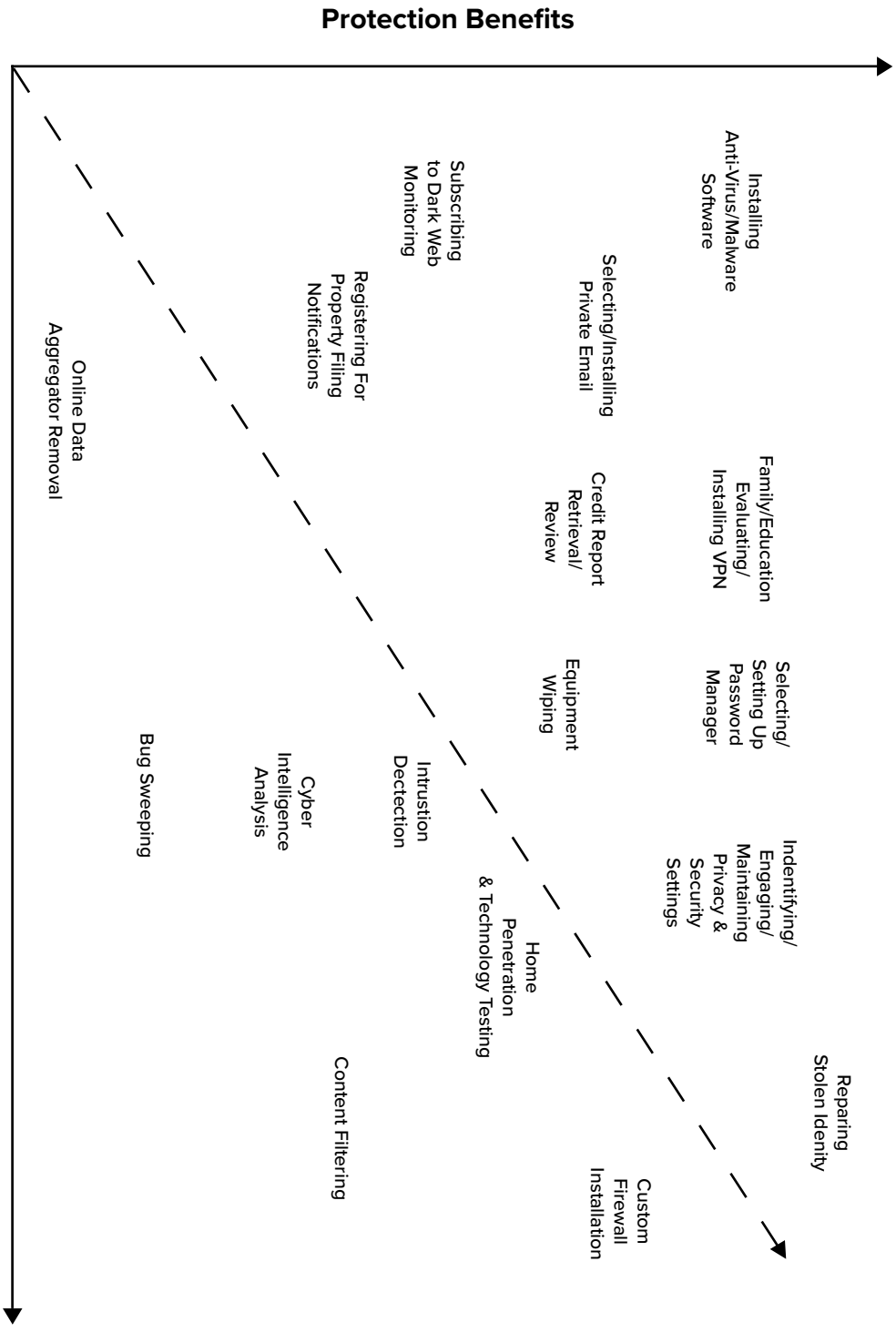
Waiting for the inevitable or capitalizing on the opportunity

The last part of the framework for managing client cyber risks involves how and when to adopt these services. We believe that it is likely that industry participants will approach this issue in the same manner that they have with nearly every other major change over the last thirty years.

Small number of firms capitalized on changes over the last 30 years

For example, in the late 90s most executives did not warmly greet the idea that they would have to become much larger and more sophisticated businesses to sustain their profitability. At that time, running a wealth manager was uncomplicated and there was little to no competition. The same individuals also often were less than enthusiastic with the idea that the industry might undergo a massive consolidation.

However, a small number of firms embraced these changes as potential opportunities to build great value in their businesses and for themselves. They aggressively marketed their services, expanded their staffs to include business operators and sought out M&A opportunities to increase their scale. Many of their organizations today are among the largest industry participants and their founders have become quite wealthy in the process.


Cost/Benefit Tradeoff of Various Cyber Protection Services
Protection Benefits
Cost/Compilicated/Time Consuming For Clients
Installing Anti-Virus/Malware Software
Selecting/Installing Private Email
Subscribing to Dark Web Monitoring
Registering For Property Filing Notifications
Online Data Aggregator Removal
Family/Education Evaluating/ Installing VPN
Credit Report Retrieval/ Review
Selecting/ Setting Up Password Manager
Equipment Wiping
Intrustion Dectection
Bug Sweeping
Indentifying/ Engaging/ Maintaining Privacy & Security Settings
Cyber Intelligence Analysis
Home Penetration & Technology Testing
Reparing Stolen Idenity
Content Filtering
Custom Firewall Installation

Similarly, we believe that most executives at wealth managers will be less than enthusiastic about the idea of adding cyber risk management services to their offerings. They likely will view it simply as having to do more for clients for the same fees. Consequently, they will only add these services when they are forced to by either client demand, market forces or when they are overwhelmed from the work involved in helping clients who have experienced adverse online events.

In contrast, a smaller group of industry participants will view cyber risk management as an opportunity that they can capitalize on. They recognize that it poses a serious problem that a great number of people are very concerned about and would like help in addressing.

At the same time, it is now almost impossible for prospective clients to distinguish between the offerings of various wealth managers vying to provide their services. Everybody effectively says that they do the same thing (i.e., wealth management.) Adding cyber risk management will enable these early adopters to differentiate their offering while at the same time addressing an important and pressing problem for prospective clients.

Some firms are already distinguishing their offerings by including cyber risk management

As noted earlier, this is already happening, and some firms have even added elements of specialization to this aspect of their marketing. More specifically, their pitches go beyond just explaining how they help clients with cyber risks in general and instead also include detailed analyses of how and why certain groups (i.e., doctors vs. lawyers vs. company executives, etc.) of potential clients may be specifically targeted by cybercriminals.

Regardless, those firms that embrace managing client cyber risks will once again have an opportunity to capitalize on an inevitable change to the industry. And the remainder will (again) find themselves having to play catch up.