Confronting the Realities of Cyber Threats

A Framework and Cybersecurity Protocols for Wealth Management Firm CEOs

September 2024

Mark P. Hurley

Brian Hamburger

Carmine Cicalese

Daniel Bernstein

Bryce Washum

Douglas Garbutt

Katherine Winford

MARKETCOUNSEL®
THE ADVISER'S ADVISOR®

DIGITAL PRIVACY & PROTECTION

CYBER CIC

Mark P. Hurley is the CEO of Digital Privacy & Protection, LLC (DPP). Brian Hamburger is the President & CEO of MarketCounsel Consulting, LLC (MarketCounsel). Carmine Cicalese is the President of Cyber CIC, LLC and Senior Partner at DPP. Daniel Bernstein is Chief Regulatory Counsel of MarketCounsel. Bryce Washum is a Senior Partner, Douglas Garbutt is Partner-in-Charge of Implementation, and Katherine Winford is a Shareholder and Director of Operations of DPP.

Contents

Introduction

Wealth managers face a new reality. Cybercrime will soon be a $10.5T annual business – larger than the sale of all illegal drugs worldwide, combined[1] – and industry participants and their clients are compelling targets. Numerous firms have already been attacked and millions of dollars of client assets have been stolen.

Wealth managers are compelling targets for cybercriminals

The U.S. Securities & Exchange Commission (SEC or Commission) along with many state regulators have made it clear that they expect industry participants to have cybersecurity protections in place. That position has been communicated through proposed regulations, examinations and risk alerts. It's anticipated that new regulations will require wealth managers to adopt cybersecurity policies and procedures that are ***"adequate"*** and that they must ***"effectively certify."*** And should the policies and procedures prove to be ***"inadequate,"*** they could face a ***"Commission enforcement action."***

This report is designed to provide a framework to help wealth management firm CEOs better understand their organizations' risks and obligations and the specific steps that they need to take to protect themselves. Unfortunately, as reflected in several industry surveys, to date most participants have largely ignored cybersecurity. Although the good news is that an effective program for most firms is neither complicated nor expensive, more than a few readers likely will be surprised by the scope and number of measures required to adequately address these threats. However, it is 2024 and not 1994 and the world is a very different place than it was thirty years ago. In fact, the cybersecurity world changes every year.

Over time, the SEC will develop its own views and policies as to what constitutes industry "best practices." And while the Commission may struggle to keep pace with rapidly evolving cybersecurity threats, wealth managers will nonetheless have to be responsive to change. Thus, our recommendations solely serve as starting points that should be independently considered to determine if they are appropriate for a specific firm at a specific time.[2]

Two foolish notions about cybersecurity permeate the wealth management industry

Additionally, it is important to dispel upfront two foolish notions about cybersecurity that widely permeate the industry. First, many executives and owners assume that it can largely be addressed by acquiring the right technology. Certainly, having good technology is a precondition to effective cybersecurity.

---

[1] https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/

[2] The provided cybersecurity protocols are CSF Tier 4: Adaptive approaches that use "risk-informed policies, processes, and procedures to address potential cybersecurity events." The NIST Cybersecurity Framework (CSF) 2.0, National Institute of Standards and Technology (NIST), U.S. Department of Commerce.

That said, this assumption ignores that it is almost always the intersection of humans and technology that creates the best opportunities to penetrate cyber defenses, regardless of the technology employed. And the success of any cybersecurity program depends heavily on the behavior of individual stakeholders.

Second, many industry executives also feel that it is inappropriate for their organizations to get "involved" in either their clients' or employees' personal cybersecurity. This notion is analogous to a pig believing that it is inappropriate for it to get "involved" in a ham and egg breakfast. Just as it is the farmer and not the pig who makes that decision, cybercriminals have stripped wealth managers of the option of disregarding personal cybersecurity.

Easiest way to breach a firm is through its clients and employees working remotely

More specifically, the easiest avenue for breaching any firm is through its clients and its employees working away from the office. Indeed, a recent study found that 82% of all financial services company breaches were initiated through employees working remotely.[3] And nearly every wealth manager has already been subjected to indirect cyberattacks involving client online accounts, email applications being chief among them, albeit deep fakes are increasingly being used. Consequently, any strategy that does not proactively address the personal cybersecurity of both clients and remote working employees will be ineffective at best.

This report is broken into four parts. The first provides essential background information for CEOs including: (i) three core concepts that underpin every successful strategy; (ii) who the bad guys are and what they are after; and (iii) what the SEC's anticipated rules obligate wealth managers to do.

The second part describes how cybercriminals attack wealth managers. It looks at the most common tactics and where firms are most vulnerable.

The third part details the foundational cybersecurity defenses that every industry participant, regardless of size and business model should consider. As their name implies, these measures are a precondition to having an effective cybersecurity program.

The fourth part provides detailed protocols that spell out the additional steps that wealth managers will need to take, depending upon their business model.

There is even now a YouTube video for creating deep fakes for Zoom calls

However, it is essential to recognize that new threats are constantly emerging. For example, eighteen months ago the idea of "deep fakes" with cloned voices and images of individuals seemed farfetched. Today, their use by cybercriminals in social engineering attacks is widespread. There is even a YouTube video that provides step-by-

[3] https://www.helpnetsecurity.com/2022/02/07/work-from-home-cyberbreaches/

step instructions for creating clones that can be used on Zoom calls. Over time other new, creative ways of attacking wealth managers will likewise emerge and they will have to respond.

As a whole, this paper spans issues, practices and recommendations that range from regulatory imperatives to risk mitigation measures to aspirational safeguards. Industry participants can use them to choose a solution set that best meets their objectives based upon the risks to their practice and their risk tolerance. We hope this, at the very least, increases awareness of the threats and potential remedies available.

Mark P. Hurley

Brian Hamburger

Carmine Cicalese

Daniel Bernstein

Bryce Washum

Douglas Garbutt

Katherine Winford

Part I – Background Information

Before trying to formulate a cybersecurity program for their organizations, it is essential that wealth management firm CEOs first understand (i) three core cybersecurity concepts; (ii) who the bad guys are and what they are trying to steal and (iii) industry participant obligations under SEC expectations and anticipated new rules.

A. Three core cybersecurity concepts

Three core concepts underpin every successful cybersecurity strategy:

1. Everything connected to the Internet will at some point be breached, regardless of what they do.

Each cybersecurity step has a marginal benefit and cost

As pointed out by a former FBI Director, only two types of companies exist: "Those that have been hacked and those that will be."[4] At the same time, cybercriminal behavior is driven by their own cost/benefit analyses tied to how much time and resources are required to breach a company versus the value of what can be stolen from it.

2. Cybersecurity is therefore an exercise in risk management and resource allocation.

CEOs must balance risk with what they can & want to spend

Because every organization will inevitably be breached at some point, the objective is to minimize how frequently this occurs and – more importantly – the accompanying damage. CEOs must balance the level of cyber risk that their firm can bear with what they can and want to spend on cyber defenses.

More specifically, just as people in the Middle Ages protected themselves by building castles with higher and higher walls and some added boiling oil and moats and occasionally even alligators to the moats, each cybersecurity step likewise has both a marginal benefit and cost. The challenge is determining the most effective cost/benefit ratio given the likely threat.

3. Damage minimization is as important as reducing the likelihood of being breached.

It is a disaster if client assets are lost

The inevitability of a breach also makes identifying and implementing steps to minimize potential resulting damage an equally important aspect of an effective cybersecurity strategy. Indeed, it is one thing to be breached where a small portion of the information for a small number of clients is stolen. It is another if entire tranches of client records are taken.

---

[4] https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies

And it is a disaster for wealth management firms if any client assets are lost.

B. Who are the bad guys and what are they after?

Cybercriminals can breach anything they target

Cybercriminals who target wealth managers can be generally divided into two groups. First, several nations' state-backed or state-tolerated cybergangs operate openly in China, Russia, Iran, and North Korea. They are run by individuals who, by day, are intelligence or cyberwarfare officers attacking Western institutions and, by night, moonlight as criminals. They have demonstrated the ability to breach anything they target including cloud services, blockchain and even US government institutions such as the DOD and CIA.

Also, thousands of smaller cybergangs operate in every country in the world, including many in the United States. Although they lack the processing power and some of the capabilities of nations' state-backed entities, they too are very sophisticated.

What are they trying to steal?

A single client data set can be sold for $1,000

Both groups are after client information and assets. Stolen client non-public personal information (NPPI) can be used for identity theft – now a $54 billion annual industry[5] – and a single client dataset can be sold for about $1,000.[6]

Additionally, cybercriminals target liquid assets that can be wired out of client accounts. They penetrate company systems or pose as clients or employees to initiate fraudulent transactions and/or alter legitimate ones.

They also try to extort money directly from wealth management firms by taking control of their systems until they are paid a ransom. Indeed, eighty-two percent of ransomware attacks are on small to midsized businesses.[7]

C. Key obligations under the proposed cybersecurity rules

As noted earlier, the SEC's proposed rules impose several new obligations on wealth managers, including six key ones:

1. Having ***"adequate"*** cybersecurity policies and procedures or risk an enforcement action

---

[5] https://www.fincen.gov/sites/default/files/shared/ID%20Theft.pdf
[6] https://www.insurancebusinessmag.com/us/news/breaking-news/revealed--how-much-is-personal-information-worth-on-the-dark-web-444453.aspx
[7] https://tech.co/news/82-of-ransomware-attacks-target-small-businesses-report-reveals

The rules would require every firm to have policies and procedures that are ***"reasonably designed to address cybersecurity risks"*** that must be reviewed and updated annually.

Wealth managers with inadequate cybersecurity risk potential SEC enforcement actions

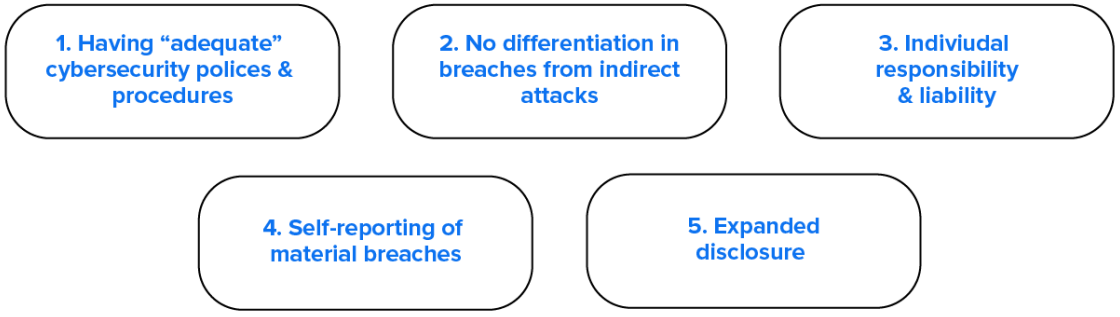
The proposed rules are also unambiguous regarding the SEC's view of those registrants that it concludes operate with ***"inadequate"*** cybersecurity. They specify that wealth managers are required to ***"effectively 'certify' their own cybersecurity policies"*** and should they be ***"inadequate," "the registrant faces down-side risks .... (i.e., Commission enforcement actions)."***

2. No differentiation between breaches resulting from indirect and direct attacks

The proposed rules do not distinguish between breaches resulting from direct or indirect attacks. This is potentially problematic for wealth managers because – as we will detail in the next part of this report – they are far more likely to be breached indirectly through clients and remote working employees than through direct attacks on their systems.

Indeed, the rules anticipate such indirect attacks. Wealth managers would be obligated to have ***"effective security practices"*** for ***"mobile or other devices approved for remote access"***... ***"whether firm-issued or personal devices."***

Five New Key Cybersecurity Obligations



Every firm has a compelling interest to mandate employees and encourage clients to operate online with better personal cybersecurity

What all of this means is that irresponsible personal online behavior by clients and employees poses a direct threat to wealth managers. And every firm now has a compelling interest to mandate employees and to encourage clients to operate online with better personal cybersecurity including better internet hygiene practices and overall awareness and knowledge.

3. Individual responsibility and potential liability

The proposed rules are also clear that the SEC views cybersecurity as not just the responsibility of firms but also of employees. They mandate ***"standards of behavior for individuals"*** and emphasize that cybersecurity is the ***"responsibility of many individuals within an organization."***

Consequently, should a firm experience a material breach, it is likely that the employees involved as well as the organization will be held responsible and are at risk of an enforcement action.

4. Self-reporting of material breaches

Firms must turn themselves in if breached

RIAs are required to self-report any material breaches to the SEC within 48 hours of being detected. Consequently, unlike other regulatory violations that examiners might uncover during a periodic examination, wealth management firms must instead immediately turn themselves in.

5. Expanded cybersecurity risk disclosure obligations

The proposed rules obligate wealth managers to ***"in plain English, describe cybersecurity risks that could materially affect the advisory services they offer."*** They must also ***"promptly"*** disclose any material breaches to clients. What happened, why, the resulting damage, and whether it resulted in an enforcement action against the firm and/or its management will become a permanent part of its Form ADV given to all current and future clients and prospects.

Wealth managers will have to inform clients that money stolen from custodial accounts is unlikely to be reimbursed

These requirements have two key business implications for every industry participant. First, wealth management firms must inform clients that, should their custodial accounts be breached, it is unlikely that any stolen money will be reimbursed.

More specifically, the most obvious potential cybersecurity counterparty risk from using a wealth manager's services is that it might be breached, and client information and/or assets stolen. Firms will be required to spell out these risks in their Form ADV Part 2 along with the steps that they have taken to mitigate them.

In addition, clients must use a custodian – typically selected from a list provided by the advisor – to avail themselves of a wealth manager's services. As a condition, clients must execute account

agreements with asset custodians that often force clients to bear the preponderance of risk of any cybertheft.[8]

Consequently, the proposed rules place wealth managers in the uncomfortable position of having to inform clients that, should their custodial accounts be breached, and they are even only indirectly at fault, it is unlikely that any stolen assets will be reimbursed. Certainly, this will be surprising if not stunning to most clients, who often equate having their assets held by a custodian like having money at a bank.[9]

A material breach could threaten a wealth manager's long-term prospects

The second, far more problematic implication of these obligations is that a material breach could also potentially fatally damage a wealth manager's long-term business prospects. Indeed, even if a breached firm somehow manages to avoid an enforcement action, the breach, its cause, and the associated damage must be disclosed to every current and future client.

Because wealth management is an industry that relies on client trust, having to make such embarrassing disclosures would be a devastating blow to any firm's long-term prospects.

6. Obligation to protect against "insider" threats

The proposed rules also obligate wealth managers to ***"develop and implement cybersecurity policies and procedures designed to mitigate"*** cybersecurity risks from insiders (i.e., rogue employees, vendors, etc.) Consequently, firms will have to limit who can access client information by type. They will have to carefully monitor new and departing employees as well as diligence vendors. They must also control access to different areas of their offices and limit what information could be stolen.

---

[8] One such agreement releases the custodian from liability should clients fail to "safeguard" their "login ID, password, or any other information used ...to authenticate [them]." Another only reimburses losses "occurring through no fault of [clients]" and only if clients "use unique username[s] and password[s]" for their accounts" and reserves the right for the custodian to "determine ....any reimbursement amounts" And a third such agreement holds clients "solely responsible for safeguarding and keeping confidential [their] passwords and user IDs" and relieves the custodian of any liability resulting from "loss or damage arising from any activity that occurs via the use of" clients' passwords and/or user IDs."

[9] Ironically, this expectation is based on a false assumption because most online banking agreements likewise force clients to bear the preponderance of the risk of cybertheft from their accounts.

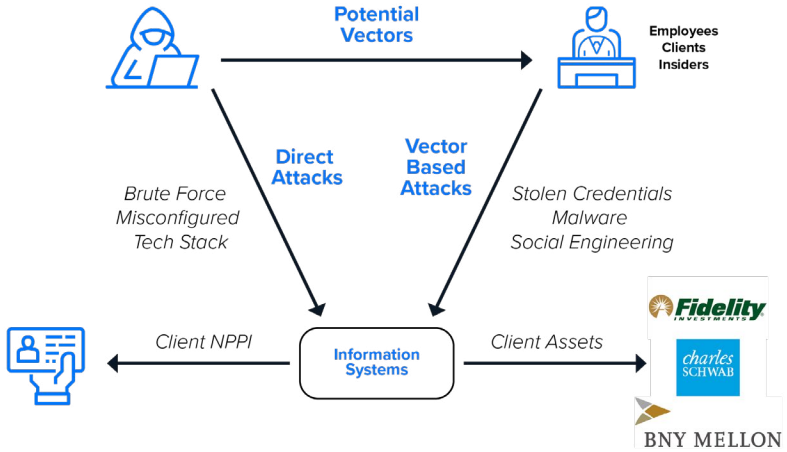
Part II – How Cybercriminals Attack Wealth Managers

Cybercriminals attack wealth managers and their clients using a variety of tactics that are constantly evolving. And the rate at which cybercriminals are innovating is breathtaking.

Rate at which cybercriminals are innovating is breathtaking

They penetrate company systems and steal client information. They also purloin credentials for accessing custodial accounts and then pose as either the client or wealth manager, initiate fraudulent transactions, and intercept the subsequent communications confirming their legitimacy.

Figure II.1
How Wealth Managers Are Attacked



Cybercriminals also have been early adopters of artificial intelligence (AI) software and have used it to create so-called "deep fakes" – very accurate clones of individuals' voices and images.[10] They are regularly used as part of "social engineering" tactics – i.e., the use of deception to manipulate individuals into performing actions – posing as either employees or clients after breaching their personal email and/or text messaging accounts, social media accounts and/or home networks. They also use AI to quickly read numerous emails and text messages from breached accounts and then initiate messages to wealth managers that are infected with computer viruses or malware.

Deep fakes are regularly used as part of social engineering attacks

[10] Eleven Labs, a software company, now offers AI technology that allows anyone to clone voices using videos and costs $4.95 per month. https://elevenlabs.io/

Indeed, criminals employ so many different tactics it is hard to keep track of them. However, they generally can be divided into two groups – direct and indirect attacks. As shown above in Figure II.1, cybercriminals either go directly after wealth managers or indirectly attack them using ***"vectors"*** – i.e., use someone who interacts with the company's systems – to breach them.[11]

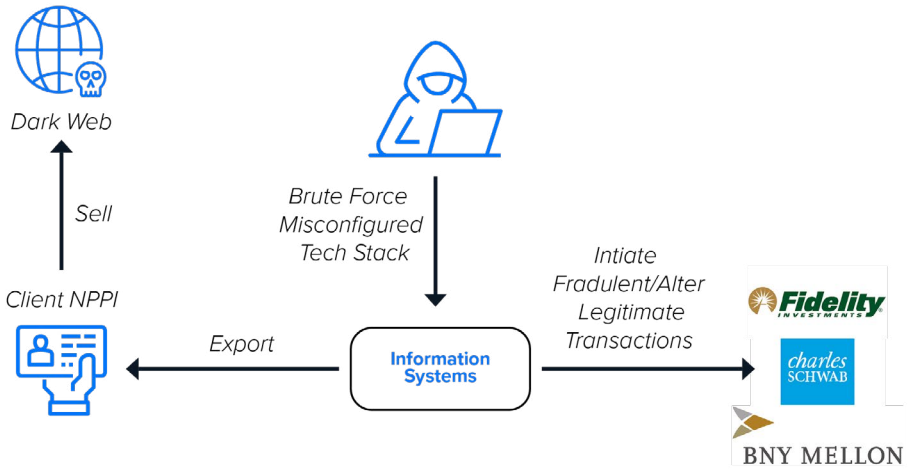
Direct attacks

Cybercriminals seek out and directly attack weak points in company systems resulting from misconfigured tech stacks or short and/or unsophisticated passwords. The former often occurs when IT staff do not change default passwords or use common ones across devices or software.

A recent study showed that computers can now correctly guess eight-digit alphanumeric passwords is less than one second

Additionally, approximately one million passwords are compromised every week[12] because it is relatively easy to use computers in what are called ***"brute force attacks"*** to correctly guess short and/or unsophisticated passwords. Indeed, a recent study showed that a computer using ChatGPT was able to correctly guess an eight-digit alphanumeric password with upper and lowercase letters, numbers, and symbols in less than one second.[13]

Figure II.2
Direct Attacks



[11] For purposes of wealth manager cybersecurity, both employees and clients are effectively "users" of company systems whose behavior can help "reduce IT vulnerabilities." NIST SP 800-50 Section 1.5.5.
[12] https://www.secplicity.org/2021/05/04/2021-world-password-day-how-many-will-be-stolen-this-year
[13] https://www.hivesystems.com/blog/are-your-passwords-in-the-green

Cybercriminals also directly attack company systems using ***"malware,"*** malicious software that is designed to get behind a wealth manager's cyber defenses, export confidential client information, initiate fraudulent transactions, alter legitimate ones, and even take control of company systems. There is an around-the-clock arms race between the cybercriminals who create malware and developers who provide antivirus and firewall software and patches against anomalies and vulnerabilities. Some days the developers win, and on others they do not.

Company systems are regularly infected when employees click on links in phishing emails or in smishing texts – i.e., fraudulent emails and texts which have either attachments or links that include malware. Many devices are also infected through ***"Trojans"*** – realistic-appearing applications that include malware – downloaded onto them either unknowingly by their owners or by criminals when a device is left briefly unattended at a conference or a resort hotel.

Infected devices can infect company systems

Unfortunately, every system can both be infected by and infect any device that is connected to it. Thus, an employee device – work or personal – that was infected while connected to an improperly protected home or other outside network could subsequently infect an employer's systems when the device reconnects to it.

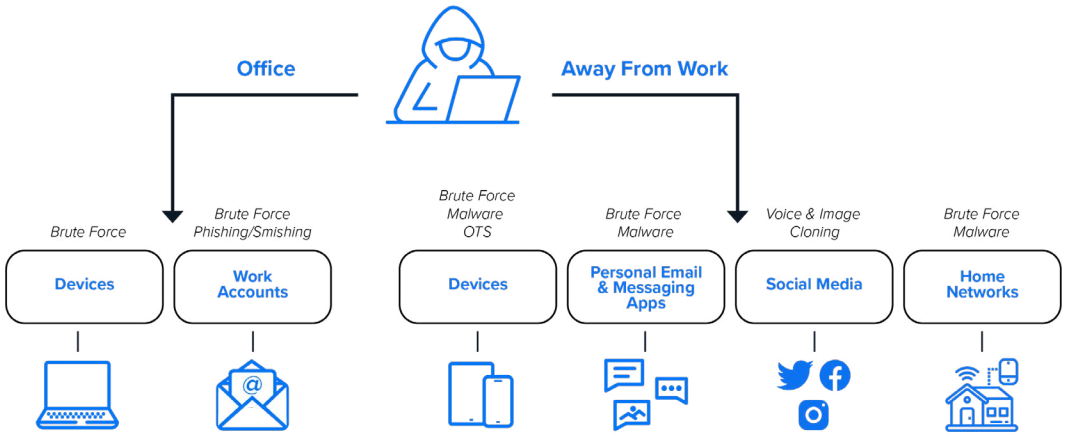
Indirect attacks

Far easier for cybercriminals to indirectly breach wealth managers

However, it is far easier for cybercriminals to indirectly breach wealth managers by targeting vectors. Unfortunately, most clients and employees who work remotely operate online with poor to nonexistent personal cybersecurity. And insiders – i.e., rogue employees, untrained employees, vendors, etc. – can easily misuse their access to the company to steal information and assets or contribute inadvertently to a breach through poor processes.

As shown in Figure II.3 below, bad actors have more ways to target employees away from work than when they are within the office environment. Online account credentials are often stolen by compromising the personal devices of employees through either brute force attacks or malware.

Figure II.3
Employee Attacks



Default settings automatically record user credentials

The default settings for most devices as well as certain Web browsers and search engines automatically record the user IDs and passwords for each account accessed. Thus, by breaching a device that is not properly protected, cybercriminals can access the credentials for hundreds of accounts.[14]

Notwithstanding, the easiest way for cybercriminals to breach an employee working remotely is through smart home technology connected to a home network. Security cameras, doorbells, and other connected devices offer entry points into the home network. Breaching a single device can effectively compromise everything – including work devices – connected to the system. Cybercriminals can then change passwords from apps and accounts and will infect devices connected to the network.

Breaching a single device connected to a network effectively compromises every other connected device

In addition to brute force attacks and malware, cybercriminals will target devices through over-the-shoulder ("OTS") or "shoulder surfing" attacks, watching an unsuspecting target enter their passcode at a public place, stealing the device, and then changing the passcode. In a matter of seconds, the criminals have locked their victim out of their own device and then begin accessing other accounts – including work ones – and changing passwords.

More recently and as mentioned earlier, cybercriminals are also downloading videos from employee social media to create incredibly accurate clones of voices and images.

[14] This includes the passwords for password managers being used by the employee.

Cybercriminals do not have to breach social media accounts to access them

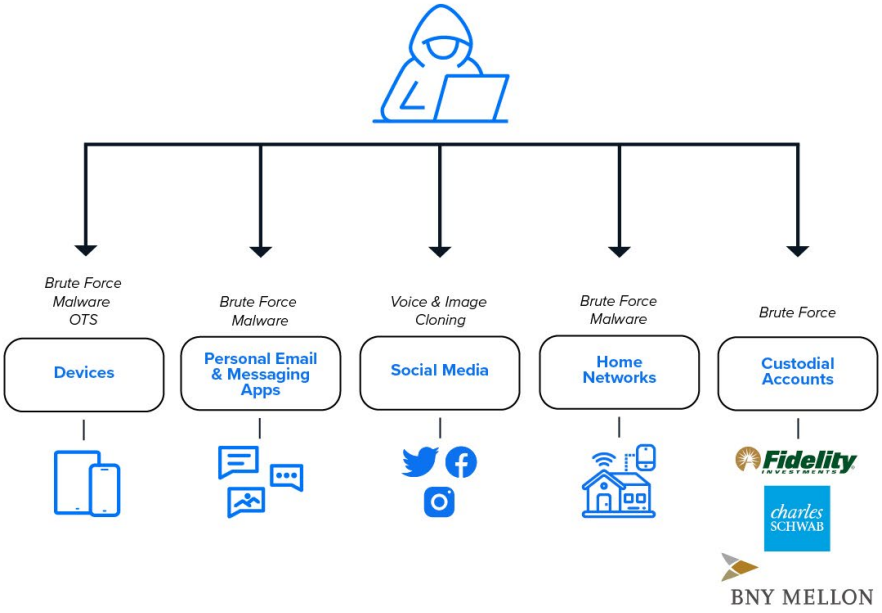
However, they do not have to breach any accounts to access this information. Rather, unless one has engaged the necessary account privacy settings, this information is out there for anyone to examine and download.

Moreover, provided they have also breached the employee's mobile device or computer they can intercept any confirmatory calls without changing any account information. And deep fakes are used regularly on phone calls; there is even a do-it-yourself video guide for creating deep fakes that can be used for Zoom calls.[15]

Targeting clients as vectors

However, an increasingly used tactic involves capitalizing on clients with poor personal cybersecurity. More specifically, as shown in Figure II.4, targeting these individuals offers many similar avenues to those of remote working employees for breaching or defrauding wealth managers.

Figure II.4
Client Vector Attacks



[15] https://www.youtube.com/watch?v=16GX8SBB2Rk

Compromised client email and text messaging accounts have been used to infect wealth managers' systems

Compromised client personal email and text messaging accounts have been used to generate messages to infect their wealth manager's systems and/or initiate fraudulent transactions. Cybercriminals have also used unprotected client social media accounts to create voice and image clones and posed as clients. And like those of employees, breached client home networks are regularly used to compromise devices and online accounts. Lastly, cybercriminals also directly target client custodial and bank accounts using brute force attacks and credentials stolen from compromised devices.

Insiders

The third widely used vectors for attacking wealth managers are insiders – i.e., rogue or untrained employees, vendors and even rogue clients. Rogue employees and clients download and sell client information and/or try to steal client assets. Untrained employees and unprotected clients are also part of the insider threat when they have poor cybersecurity defenses.

New technology enables anyone proximate to surreptitiously copy hard drives

A recent report found that it is both new employees and those who have decided to depart are the most likely to steal information.[16] Additionally, cybergang members have even become employees of targeted companies just to facilitate breaching systems.[17]

Equally problematic, technology that has been around for more than a decade will allow anyone – including cleaning staff, office visitors, etc. – to surreptitiously copy information from computer hard drives while using a device such as a cell phone that is proximate to the targeted device. All they require is access to company facilities.

---

[16] https://homework.study.com/explanation/employee-data-theft-most-frequently-occurs-with-new-employees-or-when-an-employee-has-given-notice-and-is-leaving-how-can-you-deal-with-these-two-different-issues.html

[17] 2023-data-breach-investigations-report-dbir.pdf (verizon.com)

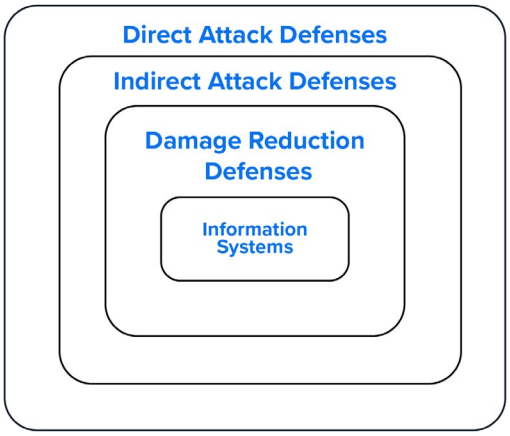
Part III - Foundational Cybersecurity Defenses

Effective cybersecurity utilizes multiple layers of defenses

An effective cybersecurity program utilizes multiple layers of defenses, each designed to address different potential threats. They are cumulative and no single layer on its own is determinative. Combined, they convert an organization into a hardened target that is far less attractive to potential cybercriminals.

The starting point for wealth management firms consists of three layers of foundational cybersecurity defenses made up of several sublayers that every participant regardless of size or business model should implement. They address both direct and indirect attacks on company systems as well as reduce potential damage from when a firm is (inevitably) breached.[18]

Figure III.1
Foundational Cybersecurity Defenses



Participants should have an annual independent review

However, these and all other cybersecurity measures should be regularly reviewed by a qualified, independent third party. The review should carefully examine whether the necessary measures have been correctly implemented as well identify any additional vulnerabilities.[19]

---

[18] This is a "threat centric," "multidimensional, defense-in-depth protection" strategy that includes "(1) penetration-resistant architecture, (2) damage-limiting operations, and (3) cyber resiliency and survivability" and addresses "dependencies among certain requirements," consistent with NIST SP-800-172 Sections 2 and 2.1.

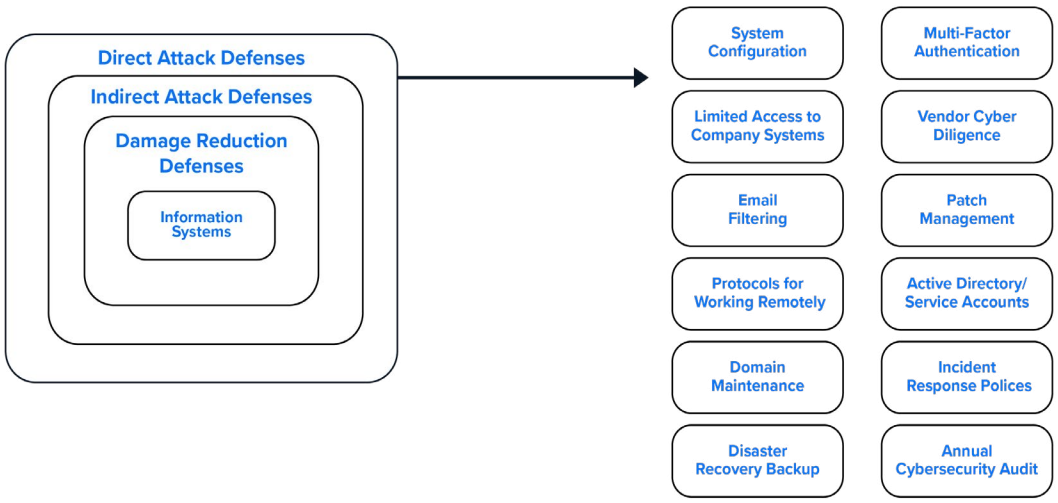
[19] It is also essential that the review's findings be protected by legal privilege because they would effectively create a roadmap that regulators could use to sanction the firm. Thus, the third-party reviewer should be retained by and provide its report to outside counsel that advises the firm on cybersecurity compliance matters.

Layer I – Direct Attack Defenses

Direct attack defenses integral to correctly functioning tech stack

Essential to defending against direct attacks are correctly constructed and maintained IT systems. The twelve steps listed below are also integral to having a properly functioning technology stack. Moreover, and quite candidly, ***should CEOs discover that they are not already in place, they should seriously consider the competency and adequacy of their IT staff and/or outsourced technology provider.***

Figure III.2
Direct Attack Defenses



Direct attack defenses have twelve aspects:

(i) Correctly configured systems[20]

Misconfigured technology is an easy avenue for breaching systems

One of the easiest ways for cybercriminals to breach a company's systems is through misconfigured portions of its technology stack. This often occurs when security settings are either not implemented or incorrectly implemented, including when the systems administrator fails to change a device or application default setting password.

[20] In aggregate, these steps "Establish configuration settings that restrict system services, provide a packet-filtering capability based on header information, or provide a message-filtering capability based on message content that reflect the most restrictive mode consistent with operational requirements." Rev 3 dated May 2024 superseded rev 2: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (nist.gov). For purposes of this report, we view client NPPI as comparable to Confidential Unclassified Information.

(ii) Multi-factor authentication[21]

All access points to company systems should require at least two different methods of authentication using one set of information that the user knows (i.e., strong password) and another thing that they have (i.e., mobile device).

(iii) Limited access to company systems[22]

Clients should only be able to connect to a separate WI-FI network

Only employees that have undergone a thorough background check should be allowed to access company systems. Even then, they should have access only to the resources they reasonably need to do their job. Those organizations that want to provide Wi-Fi access to visiting clients and/or vendors should allow them to connect only to a separate, designated network.

(iv) Vendor cyber diligence[23]

The robustness of any firm's cybersecurity is directly related to the effectiveness of its vendors. IT personnel should carefully and systematically be diligent about the cybersecurity policies, procedures and technology used by its vendors.

(v) Firewall and Anti-Virus Software[24]

Software must be systematically updated

Every system should have firewall and antivirus software that:

- Monitors end-user devices, detects and investigates threats, and provides rapid response capabilities,
- Uses machine learning to detect threats by constantly monitoring the behavior of the network for anomalies,
- Scans for signatures that are somewhat analogous to a virus's fingerprint, and
- Restricts the interaction of programs with operating systems when the program is either untested or may contain vulnerable or malicious code.

(vi) Email Filtering[25]

The company's email system should classify and categorize emails when it detects spam, viruses, and malware before it reaches a user.

---

[21] Ibid., Section 3.05.03.
[22] NIST SP 800-172 Section 3.9.1e.
[23] Diligence should include: Security Governance, Operational Security, Software Engineering and Architecture, Asset Management, Incident Management, Physical Security, Personnel Security, Information Protection, Sub-tier partner security (lower tiers, service providers, cloud) https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk- Management/documents/briefings/Workshop-Brief-on-Cyber-SCRM-Vendor-Selection-and-Management.pdf
[24] NIST SP 800-171R2 Section 3.14.2. Rev 3 03.04.02.
[25] NIST SP-800-172 Sections 2 and 2.1

(vii) Patch Management[26]

Software, drivers, and firmware must be regularly and systematically updated to protect against potential vulnerabilities. Effective patch management also helps ensure the best operating performance of systems, boosting productivity.

(viii) Protocols for Working Remotely[27]

Wealth managers should have written policies for remote work

Every wealth manager should also have a set of written policies that spell out acceptable cybersecurity practices (i.e., connecting only certain devices to company systems, when use of a VPN is required, safeguarding devices, using strong passwords, etc.).

(ix) Active Directory/Service Accounts[28]

Every device used by the company or its outsourced IT providers should be identified and user accounts should have unique permissions and privileges.

(x) Domain Maintenance

Wealth managers should also manage their Internet domains, keeping them active, registered, stable, and protected from a broad range of threats. They should also be registered privately, hiding domain contact details.

(xi) Incident Response Policies and Plans[29]

Every firm should have written policies and plans for responding to potential cyberattacks and breaches.

(xii) Disaster Recovery Backup Plan[30]

Wealth managers should also have written plans for responding to unplanned incidents such as natural disasters, power outages, cyberattacks and any other disruptive events.[31]

---

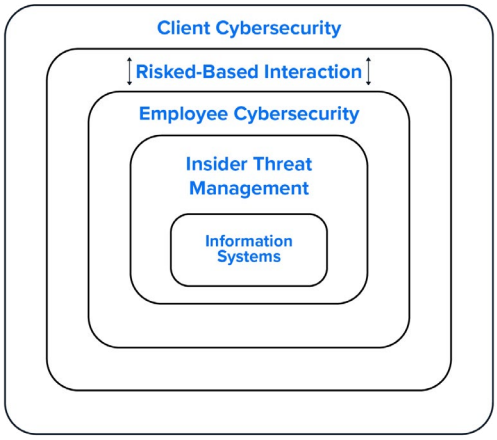
[26] Ibid., Section 3.14.4., 800-172 Section 3.4.2e.
[27] Ibid., Section 3.1.12-5,18. 800-173 Rev 3 Section 3.01.12.
[28] Ibid., Section 3.4.2. This is a common cybersecurity insurance minimum diligence requirement. Non-MS Windows devices and users can have an equivalent standard.
[29] See NIST SP 800-612 Sections 3.1-2 for the necessary elements of incident response policies and plans.
[30] NIST 800-53 Rev 5.
[31] NIST 800-53 Rev 5 CP 2. Disaster recovery backup, incidence response and business continuity plans should be synchronized.

Layer II – Indirect Attack Defenses

Largest attack surface is those points where individuals connect with technology

The second layer of foundational cybersecurity defenses reduces the likelihood of being breached through an indirect attack. As noted earlier, a wealth manager's largest attack surface is typically those points where clients, employees, and insiders intersect with technology. As shown below, there are four sublayers of indirect attack defenses.

Figure III.3
Indirect Attack Defenses



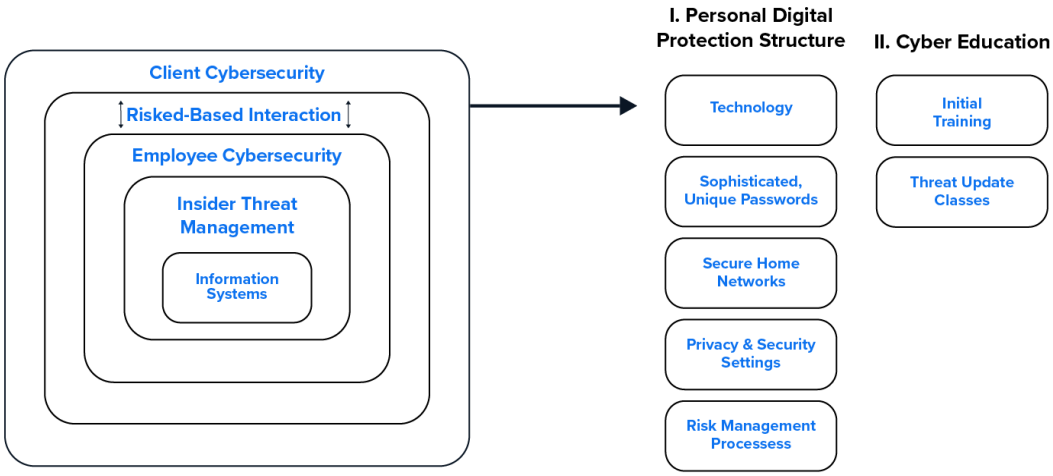
Immense difference between what firms can demand of employees at work versus the measures clients will be willing to adopt

Numerous recent attacks on wealth managers have been initiated through improperly protected client accounts and devices. Integral to defending against such attacks requires persuading clients to operate online more responsibly. That said, there is an immense difference between what firms can demand of employees at work versus the cybersecurity measures that clients (and employees personally) may be willing to adopt.

More specifically, although using cyber-protected company systems can be difficult and even frustrating at times, employees can be required to adapt to these challenges. Companies also can continuously monitor whether systems have been breached and how employees at work operate online.

In contrast, in our experience clients (and employees personally) will simply disregard cyber protections if using them makes operating online onerous. Additionally, neither are willing to invest large amounts of time or money and/or sacrifice their privacy for the sake of better personal cybersecurity.

Figure III.4
Client Cybersecurity



Both clients and employees personally will disregard cybersecurity if operating online becomes onerous

Consequently, successful personal cybersecurity programs (i) must include a set up process that is quick and painless for users; (ii) do not materially complicate a user's ability to function online; (iii) have a reasonable cost; and (iv) neither track what users do online nor allow outsiders to access any of their passwords.

They also can be broken into two groups of measures: (i) creating a personal digital protection structure for individuals and (ii) cyber education.

(a) Creating a personal digital protection structure

There are five aspects to creating a personal digital protection structure:

1. Technology[32]

Four types of technology are required:

- *Password managers (PW managers)* - Encrypted software applications used for safely storing passwords. They make it practical for individuals to use unique, "sophisticated" (i.e., randomly generated, twenty to twenty-five alphanumeric digits)[33] passwords and user ids for each online account. The user must remember only a single sophisticated password to access the software and the passwords stored within.[34]

---

[32] Unique randomly generated twenty-to-twenty-five-digit alphanumeric passwords are effectively "cryptographic keys" designed to make brute force attacks "untenable" consistent with NIST SP 800-63-3.
[33] NIST SP 800-172 Section 3.5.2e.
[34] NIST SP 800-171R3 Section 3.13.8.

- *Virtual Private Networks (VPNs)* – Software applications that encrypt online traffic between networks, preventing it from being read.[35]

- *Current Antivirus Software and Patches* – Every device should have up-to-date antivirus software. Additionally, software on devices should be regularly updated to ensure that their cybersecurity patches are current.

Anonymous email accounts significantly complicate cybercriminals' ability to change passwords

- *Anonymous Email Account* – An anonymous (i.e., does not include user's name or other information connected to them) email account that is not connected to or associated with other accounts should be used for all online accounts and for multi-factor authentication purposes. Its employment significantly complicates cybercriminals' ability to reset account passwords.

2. Sophisticated, unique passwords

Every personal online account for every member of the family should have a unique and sophisticated password that they store in a password manager.

3. Secure home networks

Every piece of technology connected to home networks should utilize a unique sophisticated password

Home networks and every device (including smart home technology) connected to them should use unique, sophisticated passwords that are stored in a personal password manager. The network should also be identified by a randomly generated alphanumeric symbol and not a family name.

4. Privacy & security settings[36]

Personal devices, browsers and search engines should be locked down by changing security settings to block the storage of account credentials and/or the exporting of information. As noted earlier, their default settings automatically record the credentials for every online account accessed, exposing them should the device be breached. The only way to prevent this from occurring is to properly set the numerous privacy and security settings on each.

Privacy settings should be engaged to control access to personal information

Security settings – including multi-factor authentication when available – also should be engaged for all online accounts. Lastly, personal online information should be minimized, and privacy settings should be engaged – in particular, on social media – to limit access to only those parties approved by the account holder. These steps make it harder for cybercriminals to target individuals, steal their identities and download videos that can be used for cloning voices and images.

---

[35] NIST SP 800-171R3 Section 3.13.8.
[36] Depending upon the applications used by the individual, there are typically between 600 to 900 privacy and security settings in aggregate that need to be engaged. NIST SP 800-128 Section 2.3.6.

5. Risk management processes

Monitoring the Dark Web provides a non-intrusive method for determining whether clients have been breached

There are three risk management processes essential to maintaining the effectiveness of a personal digital protection structure. The first is to monitor whether the structure has been breached. The most effective way of doing so without violating the user's privacy is to track if user's account information is being offered for sale.

More specifically, most cybercriminals lack the infrastructure to steal assets using compromised account credentials. Instead, they sell them in an aftermarket located on the "Dark Web", a part of the Internet used by criminals and terrorists. Should a user's account information appear there it strongly suggests that at least that account has been breached.

The second risk management process involves quickly identifying the likely source and scope of the potential breach and taking steps to remediate any potential damage. This could include resetting passwords, changing account numbers, potentially freezing credit, making filings with the FTC and law enforcement agencies and scanning devices for and removing malware.[37]

Personal digital protection structures must be systematically updated

Lastly, there should be a process for regularly and systematically updating personal digital protection structures. Companies typically change privacy and security settings on devices, apps, search engines and browsers annually. Users also get new devices that need to be locked down and retire and/or lose ones that need to be wiped. And all devices should be inspected to determine whether their operating systems and anti-virus software are up to date and if they may have been infected with malware.

(b) Cyber education[38]

Single mistake by a client could result in a firm being breached

Educating clients on cyber risks is critical to reducing the potential threat they pose to wealth manager cybersecurity. Indeed, a single, simple mistake by a client such as clicking on a malware infected link in a phishing email or smishing text might ultimately result in a firm being breached. There should be two aspects to client cyber education programs:

1. Initial cyber education

These classes should educate clients on who the bad actors are, what they are after, how they attack their victims, and the steps clients need to take to protect themselves and their families.

---

[37] NIST SP 800-61r2 Sections 3.3.1-4.
[38] Client cyber education is an essential aspect of ensuring that a wealth manager's "entire user population" has "security awareness and training" consistent with NIST SP 800-50, Chapter 2.

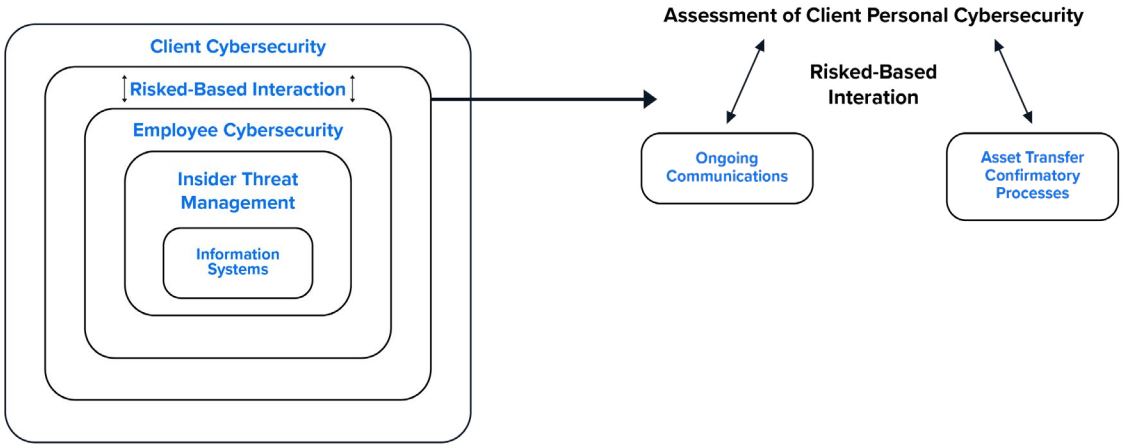
2. Threat update classes

Updates on new threats integral to client education

Cybercriminals are innovating new tactics for breaching cyber defenses at a ferocious rate. Consequently, integral to client education are ongoing classes on new threats and tactics as well as how clients can protect themselves.

(ii) Sublayer 2 – Risk-based Interaction[39]

Figure III.5
Risked-Based Interaction



Wealth managers must assess their clients' personal cybersecurity and risk-adjust their interactions with them

As noted earlier, an unfortunate byproduct of the innovation of cybercriminal tactics is that clients who operate online with poor personal cybersecurity now pose a threat to their wealth managers. Indeed, firms can no longer be certain of whom they are communicating with when working with such clients. And now even opening an email or a text message from a client risks infecting company systems with malware.

Further complicating matters is that industry participants cannot force their clients to operate more responsibly online. Indeed, many clients will not change their behavior even if their advisor offers to provide and/or pay for personal cybersecurity services.

Consequently, like the cyber diligence that wealth managers must conduct on vendors, they must also assess the personal cyber

[39] It is our view that clients with good cyber hygiene as evidenced by the personal cybersecurity steps described herein should be considered Identity Assurance Level (IAL) 2 and those who do not should be considered IAL3 consistent with NIST SP 800-63-3.

security of each client and then utilize different protocols for interacting with them based on that assessment.

Wealth managers will be able to interact with those clients who have robust personal cybersecurity in a manner that is only marginally different than they do today.

Advisors may have to require in-person meetings for some asset transfers

Unfortunately, for those clients with poor personal cybersecurity, firms must protect themselves by separately contacting them using alternative channels and personal questions to confirm their identity prior to even opening emails or text messages.[40] Advisors may also take extraordinary steps to confirm client identities – including in some instances requiring having in-person meetings – prior to initiating the transfer of client assets to new accounts or financial institutions

To be sure, these protocols cannot be static. Rather, they will also have to evolve as new threats emerge.

(iii) Sublayer 3 – Employee Cybersecurity

There are three aspects to employee cybersecurity: (i) work cybersecurity, (ii) personal cybersecurity, and (iii) training and education.

a) Work cybersecurity

Even well protected systems can be breached through how employees interact with them at work

Even well-protected systems can be breached through how employees interact with them while working at the office. Preventing this requires many of the same steps that are essential protecting personal cybersecurity. To be sure, like the direct attack defenses described earlier, *the failure to have these measures already in place would raise significant concerns regarding the competency of the firm's IT staff and its providers.*

These steps include:

- *Technology — Password managers and VPNs*

.

Work password managers should be set up so that employees can only access them using devices (either personal or work) that have been locked down.[41] Additionally, employees should be required to use a VPN[42] whenever operating online.

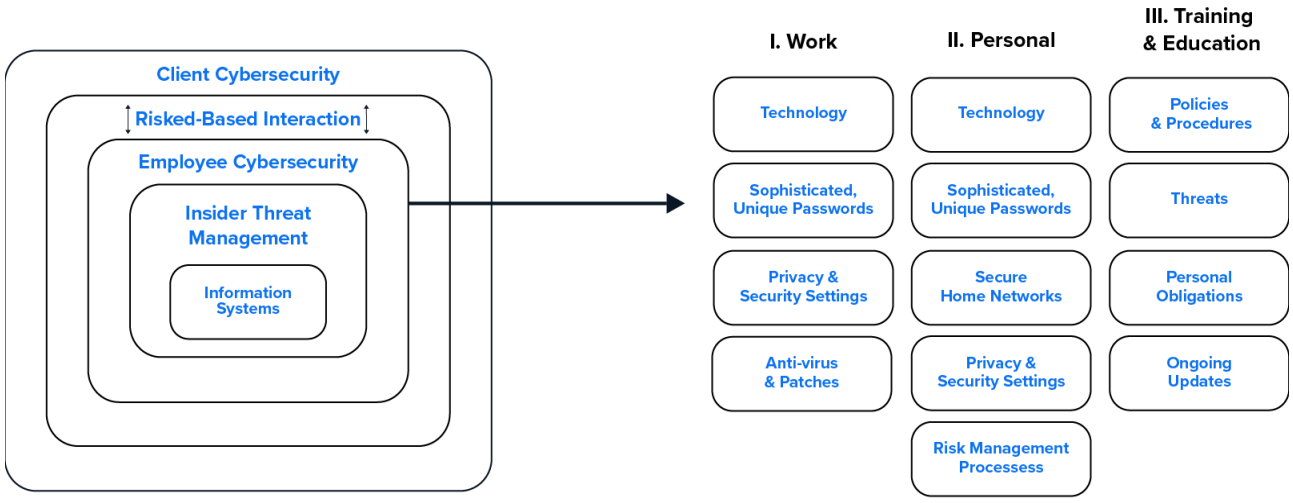
---

[40] In developing appropriate protocols for confirming client identities, wealth managers should incorporate three factors – "something you know (e.g. a password); something you have (e.g., a cryptographic key), something you are (fingerprint or biometric data)." They are the "cornerstones" of authentication systems and muti-factor authentication requires the use of more than one. NIST SP 800-63 Section 4.3.1.

[41] NIST SP 800-172 Section 3.5.3e

[42] Instead of a VPN, some companies may opt to use a remote desktop or RDP which achieves the same security goal as a VPN.

Figure III.6
Employee Cybersecurity



.

- *Sophisticated passwords*

Ideal password manager applications allow IT staff to track the robustness of work passwords

Employees should be required to use sophisticated passwords that are unique for each account. The ideal password manager applications also allow company IT administrators to track the strength of the credentials and whether the same or similar passwords are being used by an employee across multiple accounts.

- *Engaging device, search engine and app security and privacy settings on all work devices*

As noted earlier, the default settings on devices, browsers and search engines automatically record the credentials for every online account accessed, exposing them should the device be breached. The only way to prevent this from occurring is to properly set the numerous privacy and security settings on each.

- *Anti-virus and patches*

Each work device should have up-to-date antivirus software. Additionally, software on devices should be regularly updated to ensure that their cybersecurity patches are current.

(b) Personal cybersecurity[43]

The personal cybersecurity measures for clients described above should be mandatory for all employees.

---

[43] Ibid., Section 3.1.2e.

As noted earlier, remotely working employees can be used by cybercriminals to breach company systems in the same manner as clients.[44] And poor personal cybersecurity and the advent of deep fakes allows cybercriminals to pose as employees – regardless of where they are working – as part of social engineering attacks.

Employees require separate password managers for work and personal

Additionally, for several reasons employees should have separate personal and work password managers and not be allowed to use their work password manager for their personal accounts.[45] First, it is nonsensical to allow non-employee family members to access work passwords. More importantly, the more people that have access to a password manager, the greater the likelihood that it and the credentials stored within it could be inadvertently compromised.

Further, using a work password manager for personal accounts encourages employees to use them for their personal online activities, increasing the numbers and types of online sites visited and increasing the likelihood of downloading malware that could infect company systems. Lastly, using a work password manager to store personal account passwords and information also significantly complicates transitions of departing employees.

(c) Employee training and education[46]

Every employee should undergo basic cybersecurity training. They need to understand (i) how the firm is likely to be targeted, by whom and the likely tactics employed, (ii) where the firm is at most risk; (iii) the company's policies and procedures for preventing and addressing breaches; and (iv) their individual obligations.

Financial advisers play a key role in educating clients on cyber risks

Client-facing staff also should be educated on the cyber risks faced by clients, how they will likely be attacked and breached, and the specific steps they need to protect themselves. Such employees will play key roles in educating clients and encouraging them to take the necessary steps to operate more safely online.

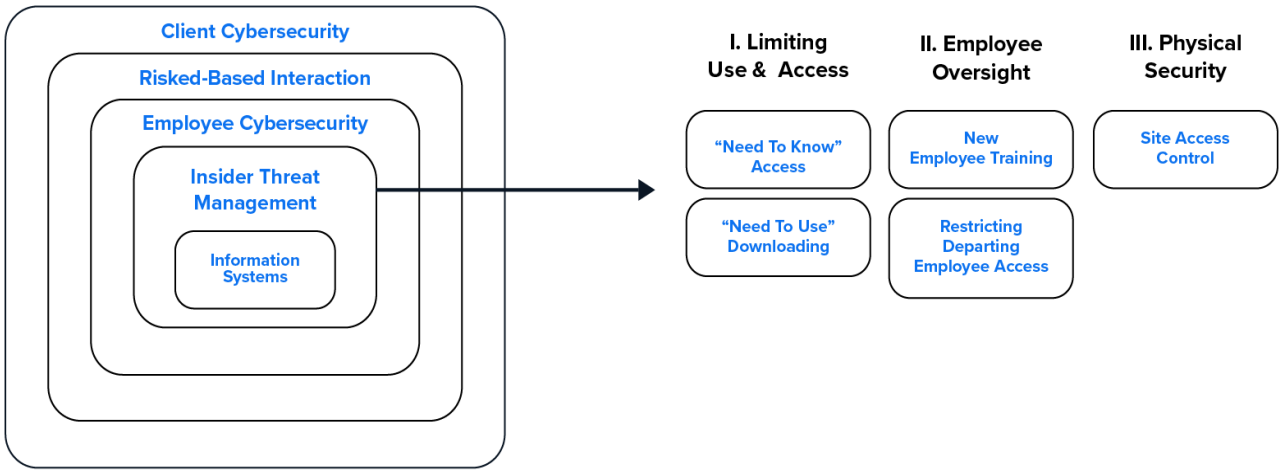
Further, employees should have regular ongoing training that updates them on new potential cyber threats to the firm and to clients. This education should include examples of how industry participants and their clients have been breached.

---

[44] NIST SP 800-171R3 Section 3.1.12.
[45] Those firms that allow their employees to include at least some personal accounts in their work password manager should only do so if the application provides for clear segregation.
[46] Ibid., Section 3.2.2.

(iv) Sublayer 4 – Insider Threat Management

Figure III.7
Insider Threat Management



Proposed SEC cybersecurity rules specifically require that registrants address potential insider threats. Wealth managers must be ***"prepared to face a cybersecurity incident....whether that threat comes from an outside actor or the firm's personnel".***[47]

We recommend six steps that firms should take to protect themselves:

(a) Limit access to information solely to those with a "need to know"[48]

Only employees who work with a client should be able to access that individual's information

Only employees who work with a client should be able to access that client's information, limiting the amount of information a single employee can steal. Additionally, access should be further limited to only the information that employees require to do their jobs.

For example, financial planners and investment team members almost never need to use client NPPI. Indeed, only compliance and administrative staff use this information. Providing access to others creates unnecessary insider risks for wealth managers.

---

[47] It is important to reemphasize that insider threats include both intentional acts as well as unwittingly acting with malice or negligence.

[48] This can also be described as the principle of "least privilege," limiting individuals' access to no higher than necessary to accomplish assigned duties. NIST SP 800-171R3 Section 3.1.5.

(b) Limit the ability to download information to those with a "need to provide"[49]

Company systems should alert IT staff of any unusually large or atypical downloads of information

The ability to download client information should be limited to those responsible for providing it to clients and for only one client at a time. Downloads should also be limited to either PDF or printed forms. Lastly, company systems should both record the authorizing employee for each download and alert senior management of any instances of unusually large or atypical data downloads.

(c) Monitor new employees' online behavior[50]

As noted earlier, new employees are one of the groups most likely to be involved in stealing client information. These individuals are also more likely to make cybersecurity errors as they learn the firm's systems and requirements. Thus, in addition to limiting their access to information, IT staff should closely monitor these individuals' online behavior.

(d) Control / limit information that departing employees can access[51]

Both new and departing employees pose insider threats

Similarly, employees who have announced their departures are also commonly involved in insider attacks. Consequently, once their intentions are discovered, their access to client information should be limited and carefully controlled. Indeed, immediately blocking their access to any client information also makes it harder for a departing employee to subsequently solicit the firm's clients or abscond with the firm's trade secrets or work product.

(e) Site Physical Access Control[52]

Devices with sensitive information should be kept in separate rooms that have controlled access

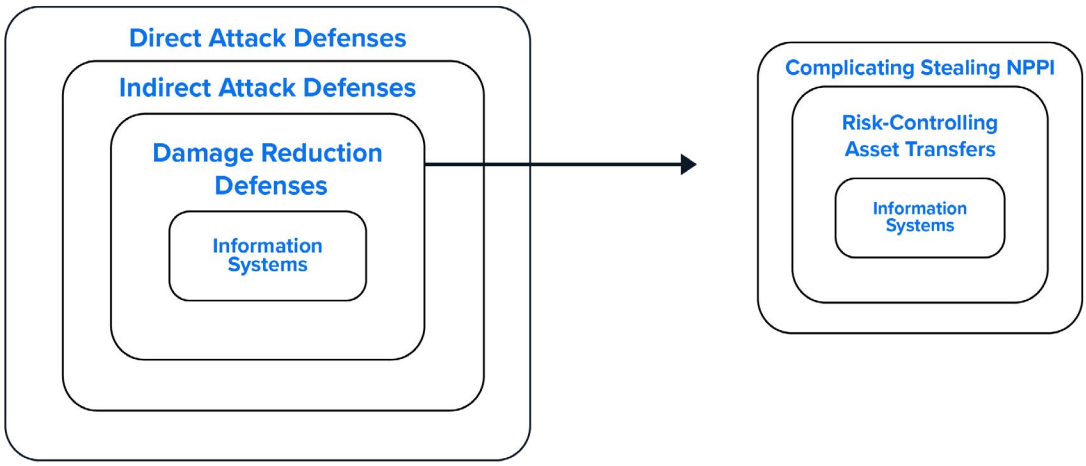
Because there is now technology that allows anyone with proximity to copy hard drives and other memory storage, devices with sensitive information should be kept in separate rooms that have controlled access. All others – vendors, cleaning staff, other employees, current and prospective clients, etc. – should be barred from entering. The devices should be kept locked and even stored in a "Faraday cage" – i.e., a shielding device that makes it much harder for someone proximate to copy their data.

---

[49] This can also be described as the principle of "least functionality." Ibid., Section 3.4.7.
[50] Ibid., Section 3.2.1
[51] Ibid., Section 3.9.2.
[52] Ibid., Section 3.10.1.

Layer III – Damage Reduction Defenses

Figure III.8
Damage Reduction Defenses



The third layer of foundational defenses address minimizing the damage from potential breaches. They include two sub-layers: (i) measures that complicate stealing NPPI; and (ii) risk-controlling client asset transfers.

(i) Sub-Layer 1 – Complicating Stealing NPPI

There are three sets of steps that wealth managers should take to complicate the ability of cybercriminals to steal client NPPI.

(a) Unnecessary Data Removal[53]

A core aspect of cybersecurity is determining what NPPI is needed and deleting the rest

Firms often hold large amounts of client personal data that they no longer need. However, should this information be stolen, it potentially could be used for identity theft. Consequently, a core part of any cybersecurity strategy is regularly assessing what client NPPI is needed to provide ongoing services and either deleting or archiving the rest.

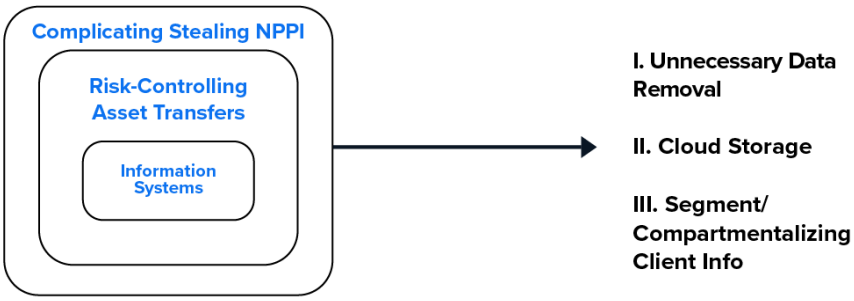
(b) Cloud storage

Unless wealth managers are willing to devote significant resources to IT systems, they should consider outsourcing as much of their information technology as possible to cloud-based companies and store confidential client data on those systems. Using them can enhance a wealth manager's cybersecurity in several ways.

---

[53] NIST SP 800-172 3.14.5e.

Figure III.9
Complicating Stealing NPPI



First, such providers typically offer and operate with multiple layers of cyber defenses and have resources for protecting information that far exceed what wealth managers can afford. Hence, unless wealth managers and their employees fail to use sophisticated credentials for accessing the systems, it is far more challenging for cybercriminals to steal client NPPI.

Using cloud services may mitigate a firm's financial and regulatory liability

Equally important, using cloud services may mitigate a wealth manager's financial and regulatory liability. Should the outsourced provider be beached directly, the loss of client information could create less financial and regulatory liability for a wealth manager than if the firm had stored the NPPI on its own servers.

Lastly, using cloud-based information services reduces the potential damage from ransomware attacks. Outsourced IT services can back up the clients' data – if engaged to do so – allowing them to quickly get back up and running should cybercriminals penetrate and infect company systems and try to extort them.

(c) Segmenting and compartmentalizing client information[54]

Most wealth manager technology systems already allow for segmentation & compartmentalization, but few use it

Wealth managers should also carefully segment and compartmentalize client information to limit the potential damage from both external breaches and insider attacks. Specifically, client information should be divided by both individual clients and the type of information. More importantly, different sets of credentials should be required to access information for certain clients and different portions of the data for that client. This type of structure limits the amount of information that can be stolen should a singleset of credentials be compromised because it limits what data can be accessed.

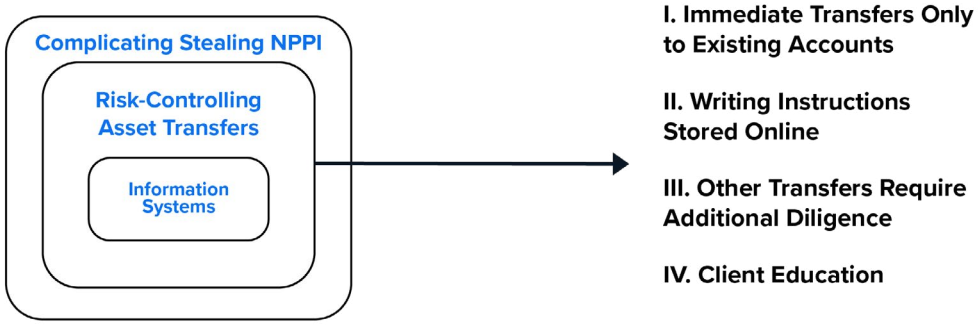
---

[54] NIST SP 800-171R3 Sections 3.13.3-4.

Somewhat ironically, we have found that the technology systems that most wealth managers already use allow for such data segmentation and compartmentalization. However, few firms have bothered to implement such controls.

(ii) Sub-layer II – Risk-controlling asset transfers[55]

Figure III.10
Risk-Controlling Asset Transfers



Cybercriminals regularly pose as clients or employees to initiate fraudulent transactions

As noted earlier, cybercriminals regularly pose as clients or employees to facilitate initiating fraudulent transactions. They have also altered legitimate ones by breaching a client's email account and changing wiring instructions at the last moment. They likewise have requested that files with client's NPPI be forwarded to them. There have even been instances where cybercriminals have set up recurring fraudulent payments from client custodial accounts.

Additionally, according to the FBI, "SIM swapping" – i.e., criminals taking over the phone numbers of their victims so that all calls and text messages are diverted – increased nearly 400% from 2018-2021.[56] Consequently, solely calling or texting a client is no longer a reliable means of authenticating transactions.

---

[55] The asset transfer control processes described herein assume that clients assessed to operate online with robust personal cybersecurity require verification measures comparable to Authentication Assurance Level (AAL)2. All others require processes comparable to AAL3. NIST SP 800-63-3.

[56] https://www.washingtonpost.com/business/2024/07/14/sim-swapping-protections-tech-tip/ca19b0f2-4196-11ef-83bf-e35a32077d3e_story.html Initially cybercriminals relied on technology that allowed them to copy SIM cards of proximate mobile devices. To protect against this, telecom companies replaced many physical SIM cards with electronic ones. However, this has not deterred criminals who often will instead target individuals with email and telecom accounts that utilize short and/or unsophisticated passwords. They first breach the telecom account and then reassign the SIM card to their number. The criminals then breach and use the victim's poorly protected email account to confirm these changes with the telecom company.

Fraudulent transactions are most successful when they are framed as "urgent"

However, cybercriminals are most often successful with fraudulent transactions that are framed as being "urgent" – e.g., a client needs money immediately. And by creating a sense of urgency, they hope that the wealth manager will take shortcuts in their verification processes. Consequently, the following four steps should be taken to prevent the theft of client assets:

(a) Provide immediate wire transfers only to preexisting, verified client bank accounts.

Wealth managers should have a bank account for each client for immediate wire transfers. The accounts should be verified long before they are needed and again each time prior to wiring funds. These accounts will provide clients with immediate access to their funds.

(b) Wiring instructions to such bank accounts should be stored offline.

Cybercriminals regularly change wiring instructions

A relatively new tactic employed by cybercriminals involves tracking potential wire transfers and at the last-minute, altering wiring instructions, redirecting funds to a fraudulent account. Unfortunately, should a company's systems be breached with malware, any wiring instructions stored online can be changed without the wealth manager even knowing. The surest and easiest means of preventing this from occurring is to store the wiring instructions for client bank accounts offline in devices that are never connected to the Web or company systems.

(c) All other transfers of client assets require substantial additional diligence that will take time.

Deep fakes & the ability to breach work and personal networks have made traditional verification processes obsolete

The advent of "deep fakes" and the ability to breach work and personal networks has made traditional transaction verification processes obsolete. Firms can no longer have confidence that they are speaking with clients or even employees when calling their cell phones or when communicating on videoconference calls.

Consequently, wealth managers must conduct due diligence on every other type of client fund transfer. This includes those initiated through employees as well as by clients as well as any new recurring payments from client custodial accounts. It also requires the use of multi-factor authentication for every transaction.

Indeed, there is a reason why individuals must often have to physically go to a bank branch and present multiple forms of identification to initiate a wire transfer of funds out of a bank account. Notwithstanding the billions of dollars spent on cybersecurity, banks recognize that they cannot be certain who they are dealing with when communicating remotely.

Additionally, firms must also – again, using multi-factor authentication – reverify wiring instructions with both the client and the receiving entity immediately prior to initiating a transaction. Doing so is essential to protecting against transaction instructions that have been surreptitiously altered.

(d) Clients must be educated

Clients must be educated on why transferring money should be cumbersome

It is critical that clients be educated on why sending funds to anywhere other than their regular bank account will involve a lengthy process, verifying the authenticity of the transaction. They need to understand that their wealth manager has an obligation to protect client assets from cyberthieves. And while the resulting process will be much more cumbersome, it is essential for protecting their assets.

Part IV – Cybersecurity Protocols for Wealth Managers

We are presenting three cybersecurity protocols for wealth managers. In addition to the foundational cybersecurity defenses, we advocate a series of incremental measures for wealth managers to consider. The specific steps appropriate for a particular firm are directly tied to how frequently it must access client NPPI and custodial accounts.

Frequency of access to NPPI and custodial accounts determines what additional cyber defenses are needed

Some industry participants – in particular, traditional wealth managers – rarely need to access client NPPI. They also infrequently trade client custodial accounts. Consequently, they can avail themselves of the Tier I Cybersecurity Protocol shown below that supplements the foundational cybersecurity defenses with only a handful of measures that make it substantially harder for cybercriminals to steal anything of value should they breach the firm. Indeed, it is nonsensical for these organizations to store certain data online because it creates unnecessary risks and different processes are better than more technology.

In contrast, a select group of other wealth managers provide one or two additional in-house services that are far narrower in scope than those provided by family offices but that do require more frequent access to client NPPI. However, these organizations also only infrequently access client accounts. Consequently, they can utilize the Tier II Cybersecurity Protocol shown below that includes additional layers of defenses but far fewer than Tier III.

Firms that require frequent access must take measures like those of large law and accounting firms

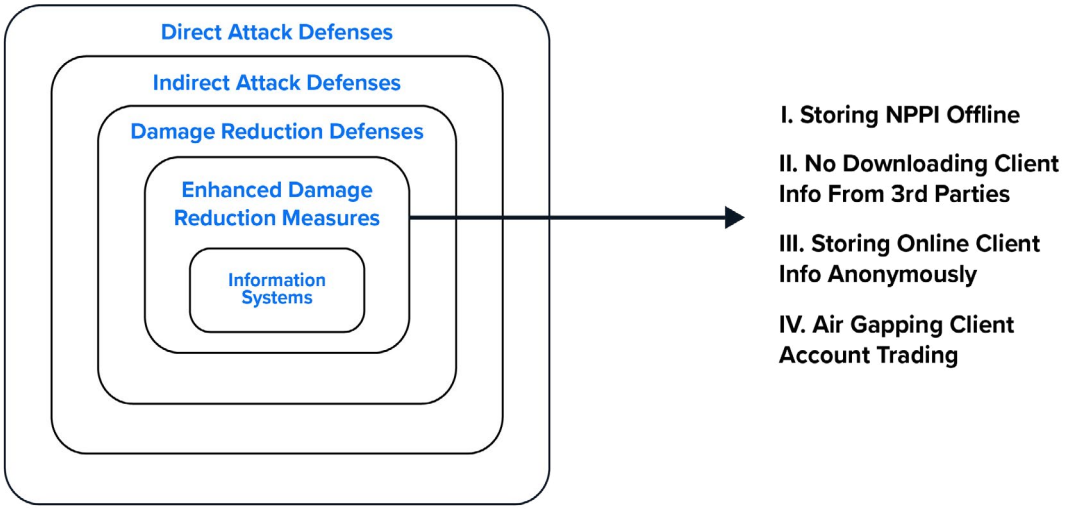
Lastly, so-called "investment counselors" and many multi-family offices typically provide a much more extensive array of in-house services that necessitate frequent access to client NPPI and custodial accounts. Many such firms actively manage portfolios of stock and bonds. Others provide in-house tax return preparation, bill pay, receivables management and/or trust services.

Thus, implementing either Tier I or Tier II protocols that are designed to make it much harder for cybercriminals to steal either NPPI or assets would be impractical – if not dysfunctional – for these organizations. Instead, they must rely on far more enhanced cyber defenses – in many ways comparable to those utilized by large accounting and law firms – that reduce the likelihood of being breached and that are detailed under the Tier III Cybersecurity Protocol shown below.

Tier I Cybersecurity Protocol

Figure IV.1

Tier I Cybersecurity Protocol



Tier I protocol is easy and inexpensive to implement

This protocol is most appropriate for industry participants that only infrequently access client NPPI and accounts (as is typical for most traditional wealth managers). It is inexpensive and easy to implement and provides robust cybersecurity. It requires – in addition to the foundational defenses – another layer of defenses made up of four steps that significantly further complicate cybercriminals' ability to steal client information and assets.

1. Storing client NPPI offline[57]

Taking NPPI offline makes it nearly impossible for cybercriminals to remotely steal it

The SEC requires wealth managers to protect NPPI which it defines as ***"any information that can be used, alone or in conjunction with any other information, to identify an individual, such as name, date of birth, place of birth, telephone number, street address, mother's maiden name, Social Security number, driver's license number, electronic mail address, account number, account password, biometric records or other non-public authentication information... or any other non-public information regarding a client's account."*** Taking it offline makes it nearly impossible for cybercriminals to remotely steal it.

All such information should be deleted from online company databases including CRMs as well as from all devices connected to

[57] These measures employ "physical separation" to "provide adequate security" while avoiding increasing the "organization's security posture to a level beyond that which it requires" consistent with NIST SP 800-171R3 Sections 1.1 and 3.13.08.

the Web or company systems. It should be stored in an encrypted database on devices kept in controlled access areas,

2. Accessing but not downloading client information from third party vendors[58]

Third party vendors such as accounting firms, bill pay services and estate planning attorneys often hold a great deal of client NPPI. A prudent step for reducing the likelihood of it being stolen is to require that employees have access to this information from vendor systems but cannot download it onto company or personal systems or devices.

3. Storing other client information in an anonymous manner[59]

Client information kept online should be made anonymous

Notwithstanding that client NPPI has been taken offline, further steps to protect client information should be implemented. More specifically, any remaining client information stored online should be made anonymous. Client names should be replaced with randomly generated identifiers. Only the employees who work with a client should know that person's identifier.

4. Air gapping trading in client custodial accounts[38]

Of all breach scenarios, the greatest nightmare for any wealth manager would involve the loss of credentials for accessing client custodial accounts. It could result in a series of fraudulent and/or altered legitimate transactions. Millions of dollars of client assets could be quickly stolen.

Every firm and custodian have safeguards including processes for confirming transactions. However, the advent of deep fakes and cybercriminals' demonstrated ability to intercept communications limits their effectiveness.

Greatest nightmare is loss of credentials for access to client accounts

That said, it is impossible to fully avoid such a nightmare scenario unless you are willing to "air gap" trading in client accounts. Specifically, only designated devices should be used for storing client custodial account credentials and for accessing these accounts. The devices should never connect to company systems and instead access the Web through a cellular connection that is shielded by a VPN. They also should be stored in a safe in a controlled access area and be shielded using a Faraday cage (to prevent data from being surreptitiously copied) when not in use.

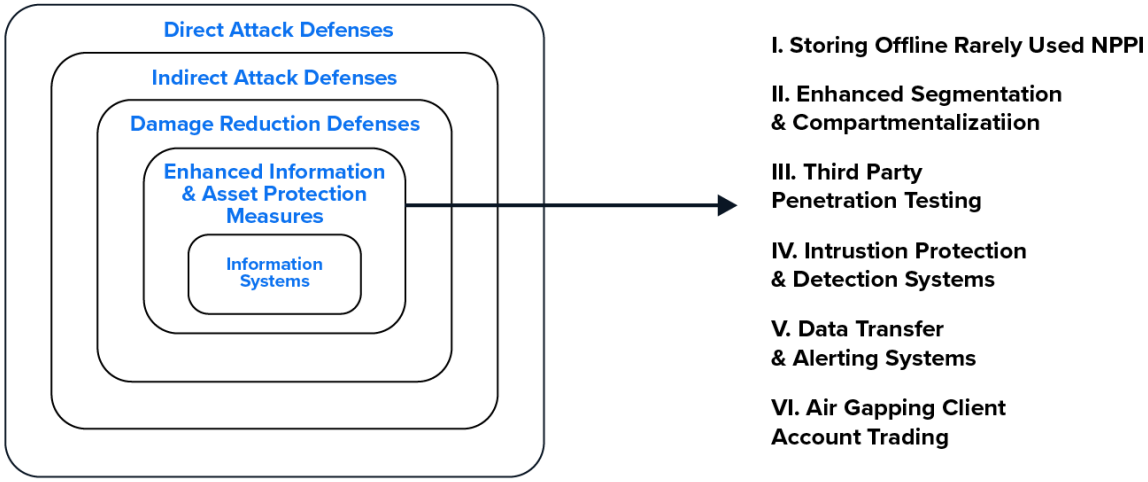
Granted, this incremental cybersecurity step limits who can trade client accounts and requires that they be in the office to do so. However, it also eliminates cybercriminals' ability to steal custodial account credentials by breaching company systems.

---

[58] Ibid, Sections 3.13.0-4.
[59] External systems such as cloud data storage require policies and procedures to protect the confidentially of client information consistent with NIST SP 800-171R3 Section 3.1.20.

Tier II Cybersecurity Protocol

Figure IV.2
Tier II Cybersecurity Protocol



At the center of the wealth management firm cybersecurity continuum are those firms that provide enhanced in-house client services. These could potentially include bill pay, receivables management and/or tax return preparation, each of which would require more frequent access to client NPPI, making air-gapping such information impractical.

As well as the foundational cybersecurity defenses, these organizations should implement six measures that reduce the likelihood of a breach and somewhat further complicate the ability of cybercriminals to steal client NPPI and assets.

NPPI that cannot be taken offline should be segmented & require different passwords to access

1. Storing Offline Rarely Used NPPI

Only client NPPI that is necessary for providing in-house services should be kept online. The remainder should be deleted from online company databases and from all company devices connected to the Web. This information should be stored in encrypted databases on devices that are never connected to the Web or company systems and that are kept in controlled access areas of the firm.

2. Enhanced data segmentation and compartmentalization of required NPPI[60]

Client NPPI that is required to provide the service and cannot be taken offline should be segmented by small groups of clients and

[60] Ibid., Sections 3.13.01 and 08.

require unique sophisticated user IDs and passwords to access. Such a structure limits the amount of NPPI that can be stolen in a single breach.

3. Third party penetration testing[61]

Firms that must keep at least a portion of client NPPI online should engage an independent party to conduct an annual penetration test of company systems to identify vulnerabilities and weaknesses in systems and recommend steps to reduce the likelihood of being breached.[62]

Relying on technology providers to penetration test their own systems is analogous to allowing bookkeepers to audit the financial records they maintain

That said, certain technology providers currently include in their offerings "AI-driven" penetration testing technology. Although its inclusion may enhance cyber defenses, it does not replace the need for an independent penetration test of company systems. Relying on technology providers to conduct such tests on their own systems is analogous to having bookkeepers audit the financial records that they are responsible for maintaining.

4. Intrusion detection and protection systems (IPS[63])

Companies that maintain at least portions of client NPPI online should also use IPS technology that monitors network traffic and searches for known threats and suspicious or malicious activity. It helps to quickly identify potential breaches when they occur and alerts the firm to block the potential breach or take other steps to reduce the likely accompanying damage.[64]

5. Data transfer alerting systems[65]

An additional layer of protection involves software that monitors activity on a network to detect any anomalies by its users, in particular involving data transfer. Such technology alerts the firm should a user's credentials be compromised and/or their device breached, and large amounts of data are suddenly exported.

6. Air gapping client account trading

Like traditional wealth managers, firms that provide enhanced in-house services should also use only designated devices for storing client custodial account credentials and for accessing client accounts.

---

[61] Ibid., Section 3.12.
[62] Like the findings of a firm's annual cybersecurity review, it is important that the penetration testing results be protected by legal privilege to preclude providing a roadmap for regulators to potentially sanction the firm. As an additional measure, the wealth manager may consider having the penetration test performed under engagement by and supervision of legal counsel that advises the firm on risk and regulatory matters
[63] NIST SP 800-171R3 Section 3.14.06 and NIST SP 800-94 Section 2.
[64] Organizations that outsource to the cloud may find that their providers do not use an IPS. They should consider upgrading to an outsourced Security Operation Center as a Service or SOCaaS.
[65] Ibid.

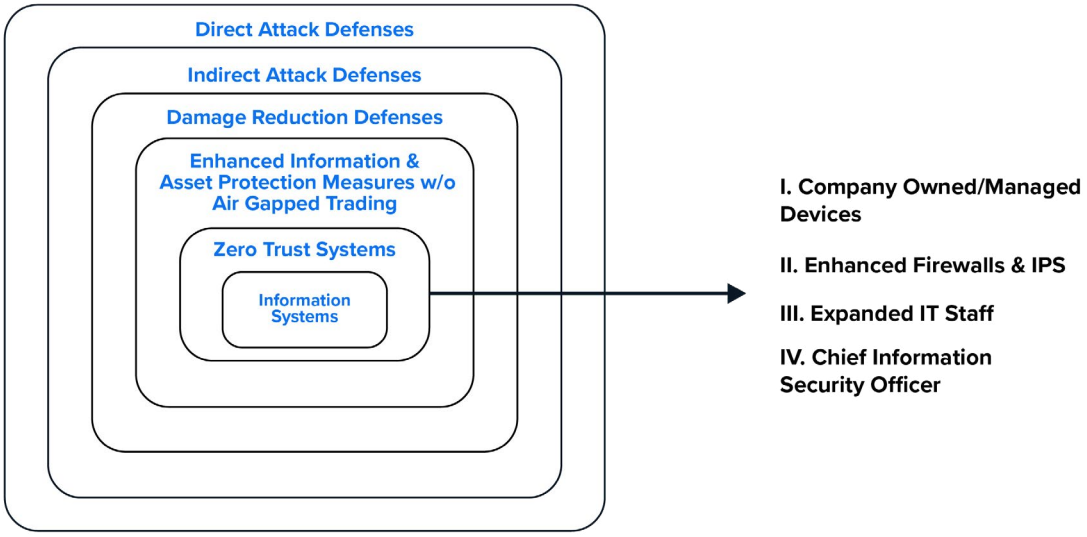
Devices used for client account trading never connect to company systems

The devices should never connect to company systems and instead access the Web through a cellular connection that is shielded by a VPN. They also should be stored in a safe in a controlled access area and be stored in a Faraday cage when not in use.

Tier III Cybersecurity Protocol

Figure IV.3

Tier III Cybersecurity Protocol



At the other end of the wealth manager cybersecurity continuum are many multi-family offices and investment counselors. As noted earlier, their service offerings require regular access to client NPPI and/or custodial accounts, making any attempt to air gap client NPPI and account trading too disruptive to their day-to-day ability to function.

Firms that cannot air gap trading must rely on "zero trust" systems

Consequently, in addition to the foundational cybersecurity defenses and the enhanced information and asset protection managers required for wealth managers with enhanced inhouse services – excluding air gapping client account trading – such multi-family offices and investment counselors must rely on “zero trust” systems that require users to be authenticated and continuously validated before accessing applications and data.

Creating such frameworks requires the following additional four measures:

1. Company owned and/or managed devices[66]

Only "enrolled" devices that are provided with several layers of cybersecurity software and settings and are remotely managed by the company or its IT provider should be allowed to access company systems. This structure helps protect the company's systems from unauthorized access and reduces the likelihood of company systems being infected with malware.

2. Enhanced firewalls & IPS[67]

Company systems with added layers of defenses operate more slowly, frustrating users

Company systems should also employ enhanced firewall and IPS technology capable of detecting and blocking sophisticated attacks and enabling a network to understand the details of traffic passing through it so it can block anything that might exploit its vulnerabilities. Adding this layer of cyber defenses often makes it much harder to access company systems and can also cause them to operate more slowly, potentially frustrating users. However, malware sophistication is increasing geometrically and utilizing enhanced firewalls is essential to reducing the likelihood of being breached.

3. Expanded IT support staff

Requiring employees to use company-managed and/or company-owned devices as well as installing additional layers of cybersecurity software will make it materially harder for employees to access and utilize company systems. It also likely will create additional hinderances on productivity. Consequently, those firms utilizing this cybersecurity protocol will also need much larger IT support staff that is on call 24/7 to help fix problems.

4. Company Chief Information Security Officer (CISO)[68]

CISOs are often the most unpopular individuals in their organizations

Zero trust cybersecurity structures are very complex and must constantly evolve to address new potential threats. Overseeing and managing them and the necessary technology vendors requires a special expertise, beyond that of typical IT professionals.

These organizations will also require fulltime CISOs who – like compliance officers – will at times be the most unpopular person in the organization. Protecting the firm will require them to implement measures that will increase operating costs while at the same time reduce productivity.

---

[66] NIST SP 800-172 Section 3.5.3e.
[67] Ibid., Section 3.14.3e.
[68] NIST SP 800-137 Section 2.4.