Building The Five Pillars Of SEC Cybersecurity Requirements As A (Registered) Investment Adviser

kitces.com/blog/sec-cybersecurity-requirements-for-registered-investment-advisors-rias

14 November 2018

Executive Summary

Over the past few years, several high-profile data breaches have hit major US corporations, including Target, Home Depot, and Equifax, bringing into sharp focus the need for individuals and businesses to protect and defend their personal data. And the matter is especially important for financial advisors, both given the importance of financially-related personal data in particular and the fact that the SEC and FINRA have been increasingly aggressive in enforcing against RIAs and broker-dealers with lax cybersecurity. And in fact, the SEC itself suffered their own data breach in 2016, despite numerous warnings from the GAO about potential security lapses.

Yet while keeping client data secure is an integral part of an RIA's compliance requirements, there's little explicit guidance from any regulatory body as to what, exactly, advisory firms are realistically expected to and need to do in order to meet those requirements.

Fortunately, there are steps that RIAs can take to develop, implement, and maintain a cybersecurity program that meets SEC requirements. In this guest post, Patrick Cleary, Chief Operations Officer at Alpha Architect, uses the concept of "brilliance in the basics," a core tenet in the Marine Corps, to explain how paying attention to basic (but important) details, being proactive, defining the specific reasons why cybersecurity is so crucial, and (most importantly) avoiding complacency at all costs, is at the core of any successful cybersecurity program for an advisory firm.

And while historically financial advisors have had to choose between either outsourcing the task of building out a cybersecurity program, or trying to decipher a mountain of regulatory material that's heavy on concept but extremely light on actionable information, Patrick details the specific steps that any advisor can take to develop a cybersecurity program. Starting with the National Institute of Standards and Technology's (NIST) comprehensive Cybersecurity Framework, Patrick provides explicit step-by-step guidance that advisors can take to understand what it is that they should really be managing in the first place, how to develop proper safeguards for client data, how to identify a breach when it does occur, and what actions to take during and after any cybersecurity events.

While there are no silver bullets, or one-size-fits-all approach or solution, the key point is to recognize that, by using the NIST framework and Patrick's actionable guide, advisors can put themselves in a much better position to protect their clients' data as well as the viability of their businesses. So whether you are looking for a framework to develop a cybersecurity program, want to stay up to date with a constantly evolving and important aspect of practice management, or want to better familiarize yourself with the subject before talking to a third-party provider, then we hope you find this comprehensive article from Patrick to be helpful!

The post goes into excruciating detail as to what you need in order to roll out a fairly decent cybersecurity program that attempts to meet all SEC cybersecurity requirements. I do not recommend sitting down and reading this in one sitting. Take every section like a chapter

and cross-reference it with your existing cybersecurity policy. If you don't have a policy yet, go ahead and build out a cybersecurity manual, one section at a time, using this post and the NIST Framework as a guide. (If you are in a hurry, you can read this post first.)

Wait a minute…NIST? What the heck is NIST? Why not just go to the SEC and download the rules???

What are the Explicit SEC Cybersecurity Requirements?

In 2016, the SEC revealed a serious, highly embarrassing security breach of their main investor database, the EDGAR system. Hackers were able to steal thousands of corporate releases and insider documents before their release to the public. The end results were over $100M in illicit trading profits and other gains at the expense of everyday investors. Despite being warned by the Government Accountability Office for…cough…EIGHT YEARS about the potential security issues, the SEC did not make the required changes, and the rest, as they say, is history.

Why am I telling you this?

The SEC, like most of us, is struggling to fully wrap their hands around cybersecurity. Imagine a police officer, on horseback, being asked to pursue criminals in cars, while simultaneously writing regulations to pursue future cars. This is the challenge the SEC faces.

This challenge is why you will not find — and probably never will find — explicit cybersecurity requirements from the SEC. Cybersecurity is changing too quickly, the government is scrambling to catch up, and posting hard "rules and requirements" like traditional securities rules could open up a slew of lawsuits. So, searching for explicit SEC cybersecurity requirements is akin to searching for the fountain of youth (see below).


Juan Ponce de León, circa 1513 searching for the fountain of youth and a comprehensive guidebook from the SEC on cybersecurity.

So…what will the SEC actually tell you? A lot, in fact. I recommend the following steps to get up to speed. Read these documents to get the SEC's general view on what they are looking for vis-a-vis cybersecurity:

1. Visit the SEC Cybersecurity page.
2. Read SEC Investment Management update on cybersecurity.
3. Read SEC IM update on business continuity plans.
4. Read OCIE 2015 Cybersecurity Exam Initiative.
5. Read sample exam checklist from 2014 from SEC (OCIE 2014). If you only have time for one, read this one.

These documents are a treasure trove of what the SEC expects and a must read for any advisor. While there is no "SEC rulebook" that explicitly tells you what to expect, these checklists and memos can give you a pretty good idea of what has been asked for in the past.

Now, how does an advisor actually build a robust cybersecurity program?

Fallujah, Iraq – the crown jewel of cybersecurity training!

I am amazed by the parallels between cybersecurity compliance and combat. Having served as a U.S. Marine from 2004 to 2008, I believe cybersecurity requires the exact same combat mindset as the battlefield.

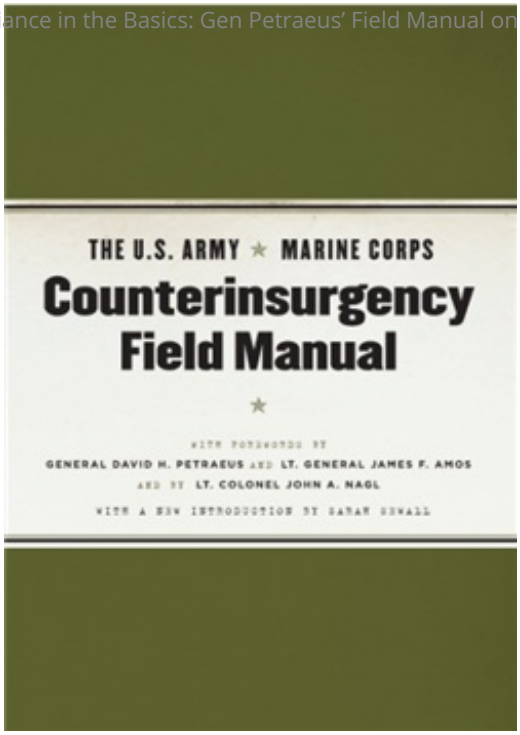
Let me explain…

One of the most striking lessons I learned in the Marine Corps was the power of "brilliance in the basics." I joined the Marines at the crescendo of the Iraq War, when America was pivoting from "shock and awe" towards a counterinsurgency fight that would be measured in years, not weeks. American technology was quickly being supplanted by traditional counterinsurgency tactics and boots on the ground.

> Train in conditions that are harder than those in combat and be *brilliant in the basics.*

I quickly grew to appreciate those words when we deployed in January of 2007 (combat engineer platoon – great gig).

Brilliance in the Basics: Gen Petraeus' Field Manual on



Counterinsurgency Operations

Despite all of the new technology the Pentagon was bestowing upon us, I found our platoon's success to be centered around four core principles:

- Explain the “why” to all levels of the platoon (What is the purpose of this mission? What is our intent?).
- Be really good at the basics (shoot, move, communicate).
- Dictate the terms of the battlefield (never let the enemy tell you where to fight).
- Complacency kills.

Explaining the “why” to all levels was essential for success. The platoon had to understand why they were being tasked with risking their lives on a particular mission. More importantly, they had to know the purpose, or Commander’s Intent, in order to act independently and take the initiative. Simon Sinek has a great piece on “The Why” that I highly recommend.

With intent clearly communicated, the “basics” of being a good Marine by far outweigh the importance of new technology or a cool piece of equipment. Maps and basic land navigation skills never required a GPS signal. Simple radios always seemed to work better than high-speed combat laptops. Observant foot patrols seemed to maneuver more easily than high tech HUM-Vs loaded with equipment.

After brilliance in the basics, we could dictate the terms of the battlefield to the enemy. If a police station had to be fortified against car bombs, we did it at night to avoid sniper fire. If an outpost needed engineer support, I would time our departures (when I could) to dovetail with armored units or IED clearing teams. Whenever we patrolled in the open, we strove to coordinate overlapping resources (air, helicopters, etc.) to ensure maximum firepower was available to bring upon any enemy we faced.

But who was the enemy we truly faced? I found myself battling complacency with more vigor than any Al Qaeda insurgent. Checking, testing, and rechecking radios, gear, weapons, patrol routes, intel briefs, and first aid kits was a daily struggle. The greatest risk to mission accomplishment was getting complacent and abandoning those tasks that would save our lives. What I envisioned combat to be as a naive lieutenant was quickly replaced with what combat largely was – a daily slog against our own internal weaknesses. This is the epitome of cybersecurity. Granted, there were split seconds of enemy engagement or other adrenaline-inducing events, but the bigger battle was the battle between discipline and disorder. Action versus inertia. Warrior mindset versus comfort mindset.

(Disclaimer: all combat experiences are different. I was lucky enough to not get shot at every day. Others were not as fortunate)

> What I envisioned combat to be as a naive lieutenant was quickly replaced with what combat largely was – a daily slog against our own internal weaknesses. This is the epitome of cybersecurity.

And so it is with cybersecurity. Plainly stated — cybersecurity requires a combat mindset.

Attention to detail, being proactive, communicating the "why" to the troops, and most importantly — avoiding complacency are critical. Financial advisors must have the right mentality to build a successful cybersecurity program — it's tough, requires discipline, and is an on-going fight. Contrary to popular opinion, cybersecurity is NOT an IT exercise that requires a Master's in computer science.

So…before you begin this mission, always remember – complacency kills!

Mission: Provide a Comprehensive Cybersecurity Guide that Any Advisor Can Use

Financial advisors today are presented with two abysmal options when it comes to meeting SEC cybersecurity requirements:

- Option 1: Hire mercenaries to fight on your behalf. Pay a king's ransom for external experts and their standard cybersecurity program.
- Option 2: Read a bunch of high-level guidance with no step-by-step instructions (e.g., "yes, I know I need to encrypt my data…how and where please?)

These were the options I encountered when building our cybersecurity program. Outsource everything or "boil the ocean" by reading lots of conceptual papers and "guides". We had to build a better way…

The mission of this post is to equip financial advisors with the tools necessary to be "brilliant in the basics" of cybersecurity and meet the requirements of the SEC. You do not need to be a computer programmer to have a solid program. You do not need to hire third-parties at exorbitant rates or pay some software startup thousands of dollars to manage your "battlespace." What you do need is a combat mindset. You will have to roll up your sleeves, get a little dirty, and most importantly, be willing to do "battle" with egos, priorities, and preconceived notions that you, your coworkers, and even your clients, may have.

Disclaimer: There is no "perfect" solution to cybersecurity and every situation will be different. Consider this blog post to be the used Hyundai of cybersecurity programs. You will certainly find problems or deficiencies with it, but it sure beats taking the bus and it's cheaper than buying a Lexus. Ongoing improvements and enhancements are a necessary and mandatory part of the program.

With that in mind: let's get after it.

Getting Started: NIST…a Compliance Officer's Best Friend

As I mention in my post on how to develop a cybersecurity program, the National Institute of Standards and Technology (NIST) is your best friend. NIST is basically the entity that ALL

government agencies and large corporations look to for guidance on cybersecurity. There is no need to reinvent the wheel or pay out of pocket for a best in class cybersecurity framework. The new release is right here for free. I strongly recommend reading this PDF before progressing any further. If you are a CCO, I also recommend reading the "markup" version so you can see what is changing over time. Version 1.1 (April 2018) has a ton of additional compliance material on vendor management. No surprise after all of the third party vendor breaches in the last few years (Target, Home Depot, Best Buy).

Most importantly, this document is what the SEC and state regulators will refer to when tailoring their Examination Priorities. For 2018, here's a hint:

> We will continue to prioritize cybersecurity in each of our examination programs. Our examinations have and will continue to focus on, among other things, governance and risk assessment, access rights and controls, data loss prevention, vendor management, training, and incident response.
>
> — SEC 2018 National Exam Program Examination Priorities , Page 9.

Broadly speaking – a best in class cybersecurity program will touch on the five key areas outlined by the NIST framework:

- **Identify:** Understand what a financial advisor needs to track/monitor/mitigate.
- **Protect:** Develop appropriate safeguards for advisor data.
- **Detect:** Implement activities to identify an actual breach.
- **Respond:** Develop responses to cybersecurity events.
- **Recover:** Implement ongoing operations to get better and reduce the impact of a successful breach.

Let us tackle each "pillar" of the NIST framework and translate it into an actionable guide with immediate to-dos. If you want to follow, refer to Table 2 of the NIST Framework. I strongly recommend you use some kind of reminder system (SmartSheet rocks, but use whatever) to keep track of all these tasks. I also strongly recommend you write these processes into your compliance manual or create a separate manual for cybersecurity. Complete these steps, grasshopper, and you will be on the path to true cybersecurity enlightenment (Kung Fu reference, FYI.)

And now, prepare to walk into the buzz-saw of DIY cybersecurity.

Pillar I: Identify (what are the rules and what do I need to track?)

Before you build a house it's a pretty good idea to have the blueprints. Our first "Pillar" of cybersecurity is the "Identify" pillar or, "What the heck am I supposed to do / where do I get started," pillar.

There are six core areas that require attention:

1. Asset Management: Identify risks and build an action plan.
2. Business environment: Identify and secure the data.
3. Governance: Write the rules.
4. Risk assessment: Review your plan and identify where it sucks.
5. Risk management strategy: Take the parts of your cybersecurity plan that suck, and make them suck less.
6. Supply chain (Vendor) management: Make sure people you pay to do things on your behalf don't suck.

I. Asset Management

Asset Management has a completely different meaning in the cybersecurity context versus the financial services context. In the cybersecurity world, "Asset Management" literally means identifying what the heck you have (e.g., computers, tablets, phones, and so forth) and who is in charge of monitoring/managing these assets. This is very simple stuff, but important.

1. CISO Nominee: Designate a Chief Information Security Officer (CISO). Most likely the poor bastard you tagged with CCO, but can also be someone else. Make your CISO responsible for everything in this post. Be sure to buy them a drink or let them sleep in tomorrow as they will hate you for the torment you are bringing upon them.
2. IS Committee: Designate an Information Security Committee (ISC). Have this committee meet quarterly or every six months. Take notes and DOCUMENT that this meeting actually happens. May seem silly, but examiners will literally ask for the memo/meeting summary notes as evidence that you are actually doing something. The mission of these meetings is to update your policies as the battlefield presents new challenges (e.g., new threats, new business lines, etc.).
3. Hardware inventory: In a spreadsheet, document all IT hardware you have (desktops, laptops, smartphones, routers). Anything with data or anything that touches data should be on this list. You will need unique identifiers (Serial numbers are good) or you can label the items yourself. Put this list in a safe place and refresh it. Whenever any new piece of equipment comes in or an old piece of equipment goes out, capture it in this list. Audit this list regularly and keep it up to date.

4. Software inventory: In a spreadsheet, you need to list all “authorized” software. Team members wanting to add a new program need to have it approved by the CISO. Write down this list and save it. Refresh quarterly.
5. Audit the hardware and software inventory regularly. Use this tip to export what software is installed on a machine. Inspect each workstation to ensure all hardware accounted for. Do this quarterly.
6. Draw a map of your network in PowerPoint. Doesn’t have to be pretty. This is literally a forcing mechanism to understand what your network looks like and what needs to be protected. This diagram will also help you discover items you may not have thought of before. Do a lot of work from home? Guess whose home computer is now on the company network map and in the inventory tracker? Refresh quarterly.
7. Take your network map and add the relevant third parties you deal with (Google Suite, TD Ameritrade, Salesforce, WordPress, whatever). The goal here is to identify where your data may travel beyond the network. Refresh quarterly. (This will be very important when we hit vendor management later on.)

Boom. Done. Now you have an inventory of data assets, a map of how data flows through your organization, and most importantly, delegated responsibility to an Information Security team to track everything. Again, none of the above is technically complex. Discipline, grasshopper, is essential.

II. Business Environment

This area of cybersecurity pertains to, “What do we do as a business and how does that generate risk?” These points are primarily addressed later on during the risk assessment phase, but they are worth touching on now. There is one main task to do here that will cover everything: write down your answers to these questions and review them during your first IS meeting (referenced above). Being able to prove to examiners you are reviewing these elements, at least annually, is a good thing.

1. Identify your firm’s role in the “supply chain.” For advisors, what do you do and where does that generate sensitive data? If you do a ton of financial planning, where does that data get stored? If you regularly partner with a CPA firm, how does that data get shared? When? Etc.
2. Identify any critical infrastructure. Critical infrastructure is typically associated with large custodian banks. That said, all firms necessarily rely on some key infrastructure or element. Have an in-house server? Do you rely on Dropbox for all of your cloud needs? Etc.
3. Identify what “resilience” requirements you need to ensure you can still function as a business. E.g., what happens if your Bloomberg Terminal gets taken out? What do you need to access your data in the cloud? Etc.

Now, notice that NONE of the requirements listed here require technical know-how. This section requires a pen, paper, and most importantly, dedicated time for thinking. I can't tell you what your business environment is, only you can. A financial advisor with four offices and internal servers will have a much different vulnerability profile ("attack surface" is the cyber geek term) than a singular home office setup. Pen. Paper. Thinking. This will be a recurring theme throughout this post.

III. Governance

Governance boils down to: "Do you have this stuff written down, delegated, and communicated to those that need to hear it?"

1. Ensure you have a cybersecurity manual in place and you distribute it to employees annually. Add annual training and document who attends. You can use the NIST framework mentioned early to write one. Doesn't have to be pretty. Just put pen to paper.
2. Congrats! You have already designated a Chief Information Security Officer (CISO) and Information Security Committee (ISC) above — a critical governance element.
3. Regularly review SEC guidance on cybersecurity, GPDR requirements (EU privacy regulations), and other bulletins that outline what you need to implement. Staying close to FINRA, NIST, and other regulatory bodies is time well spent.
4. Ensure you have a tracking system (Excel, SmartSheet, stone tablets, whatever) that track and implement your program. Set an annual review to update this system with new requirements from #3 above. Ensure a risk assessment is part of this step and you conduct it annually. I strongly recommend using the small firm cybersecurity checklist from FINRA for this.

IV. Risk Assessment

This is a critical section, with multiple tasks, but it can all be distilled into a single step: run a robust risk assessment process every year and update your program accordingly. Again...get the small firm cybersecurity checklist from FINRA. They take all the guesswork out of conducting a risk assessment and what to do with the results...

1. Identify and document your firm-specific cybersecurity risks. The small firm checklist referenced above is the template to do so.
2. Get intel from outside sources on new cybersecurity threats. The easiest way to do this is to sign up for the Department of Homeland Security's (DHS) Computer Emergency Readiness Team (CERT) listserve. This is a national initiative where the DHS looks at all sorts of new cybersecurity threats and blasts it out to everyone in the business community. A lot of these alerts will not apply to you, but every so often, CERT will publish a vulnerability in Windows, or some other common software you likely use.

You can sign up for the listserve here. (See screenshot below.)

3. Once you have your threats and vulnerabilities identified, jot down the impacts and likelihood that they will occur. E.g., if North Korean agents specifically target your firm, that would be catastrophic, but a low probability. Accidentally spilling nacho cheese on your laptop while reviewing KYC documents and frying your laptop is a medium impact, high probability event, etc.
4. Take your risks (#1), the business impacts and probabilities therein (#3), and create a list, in descending order, of the risks to your firm. Congratulations, this is called a risk assessment. The goal here is to help you determine what are the priorities for your cybersecurity program. In our example above, you are probably at greater risk of spilling nacho cheese on your laptop than having the North Koreans steal your stuff, so maybe your first focus is on having a backup system. We will focus on the North Koreans next week….
5. Take your freshly minted list of risks and write down action plans for each. Staying with our nacho cheese example:
    1. Risk — I spill nacho cheese all over my laptop, because, face it, I love nacho cheese.
    2. Impact — Spilling nacho cheese all over my laptop will fry it and cease all operations. I do not have any other backups in place because I am, in fact, an idiot.
    3. Probability — There is a high probability that I will spill nacho cheese on my laptop because I consume 2 quarts of nacho cheese per week.
    4. Action plan — We will establish a file backup system in the cloud and maintain a backup machine onsite. I will also refrain from eating nacho cheese while working and document this policy in our compliance manual.

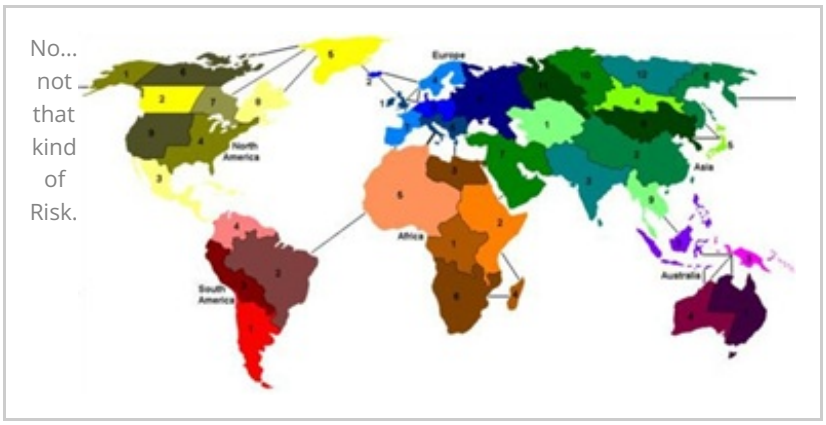
Regulators want you to stay up to date on new threats…why not let DHS tell you what to focus on (for starters).

This example underscores a key point: a third party firm cannot do all of this for you. Any consultant will tell you to back up your machines and have physical redundancy. No one would know to incorporate a “non-nacho cheese policy” into your compliance manual. Of course, this is a stupid example, but many situations exist particular to your firm’s circumstances. What if you travel 95% of the time and meet clients offsite? What if you work from home or share an office with another business? These considerations can present significant risks to your organization that no off the shelf solution will automatically identify.

V. Risk management strategy

No one can eliminate all risks with 100% certainty. The only way to do so would be to cease operations entirely. This section specifically asks the firm to document the following:

1. Document how you will do a risk assessment. I recommend outlining an annual risk management review in your compliance manual, with sign-off by the CCO every year.
2. Outline how risk is determined. The small firm checklist can be your "risk-triage" system. I recommend referencing this tool in your compliance manual.



V. Supply chain risk management

This one is a biggie. I highly recommend reading this post on vendor management. As the article highlights, weak cybersecurity policies from third-party vendors can be the Achilles heel of any cybersecurity program. To be in compliance, consider the following:

1. As part of your annual risk assessment, be sure to include considerations for every critical third-party vendor you work with (e.g., MailChimp, Dropbox, TD Ameritrade, etc.).
2. Review contracts and user agreements from these third party service providers. Identify where you are indemnified for cybersecurity breaches and for how much (if anything). Add this consideration to your risk assessment.
3. Conduct due diligence on your third-party vendors to ensure their platforms are secure (I know, sounds daunting. It isn't. Read this post).
4. Incorporate the failure/breach of a third party vendor into your business continuity plan.

So there you have it. Follow those steps and you are well on your way to having a robust understanding of your risks and what you need to protect.

Pillar II: Protect (harden your targets against attack)

Once you know the risks and what to track (Pillar I: Identify) you can now begin to fortify

Mr. Raymond James establishing a cybersecurity perimeter for his first advisory office. Circa 1957.

your positions.

There are six areas of the "Protect" pillar. Once you chew through these, you are halfway through this post and on your way to a well-deserved nacho cheese snack of your choice.

The six subcategories are as follows:

1. Access control: Let's make sure that access is given only to those that need it.
2. Awareness and training: getting employees stoked about compliance!
3. Data security: hint, it rhymes with encryption.
4. Information protection and processes: yup, it's as boring as it sounds.
5. Maintenance: let's fix our stuff in a safe way.
6. Protective Technology: use tools to keep us up and running.

I. Access Control

A revolutionary concept here: ensure that people who access your data are the right people.

Below are the steps you need to take:

1. Create an access roster. Employees on the far left column. Critical systems in the first row. Fill in this access matrix with who should have access to what. Admin assistants probably shouldn't have logins/credentials for trading platforms. Traders probably don't need access to HR materials, etc. There are a million ways to segment your access (and that, friends, is for another post), but at a minimum, you should understand who can log in to what. Also, if you are sharing passwords for certain critical applications…stop…now. Review and refresh this list quarterly. Be on the lookout for terminated employees, new employees, or current employees migrated to new roles. Those actions should trigger a credential change immediately.
2. Audit physical access. Conduct a physical audit of your assets. Is it easy to steal stuff? Does everyone have a laptop that can be taken anywhere? Do you lock the doors at night? Security system? The list goes on. Again, think common sense here. What do I need to do in order to ensure my physical assets are safeguarded? How would you notice if a laptop went missing? Put these steps in your compliance manual. For example, some firms have spare keys to the office, but may not keep track of them. Probably good to have a key roster and put that in your compliance manual. Do you maintain a server in your office? Why not add a separate door lock and keep it secured? Keep an access log of who goes in and out of the server room, etc. At the

Fed, all access to servers requires a machine gun escort!

3. Remote access. Remote access refers to someone being able to access your machine remotely. Most independent advisors do not need this capability (or if they do, it is rare). The best practice here is to adopt a policy of "disabled" remote access. That is, only turn it on when you need it, and be sure to turn it off when you don't. Larger shops may need a more nuanced policy, but the basics are here. This article gives a decent overview of how to disable remote access.
4. Access and authorizations are managed, incorporating the principles of least privilege and separation of duties. You have already touched on this with #1 (access roster). The main goal here is to limit access to only what individuals need. How this is accomplished is largely dependent upon how you store your files and access client accounts. For example, Dropbox Business has a user access feature where you can separate access to distinct users/roles. Google Drive does not have this feature, but you can limit access and share specific folders only. While we can't delve into how any particular system can be configured, we can tell you this: It is best practice to limit your team's access to what they need and nothing more. A key area that many firms mess up is failing to execute on this principle.
5. Network segregation. This activity is more relevant for larger enterprises. For a small advisory shop, it is recommended to split your network into two. Guest and User. Guests (e.g., clients that visit onsite) can have access to wifi, etc. without being granted credentials to your main network. This article is a good start, but you will likely need to make changes based on your specific networking equipment.
6. Identity verification. The key action item here is to enable two-factor authentication wherever possible (e.g., you receive a text message on your cell phone to access your email, etc.). The main objective here to ensure that people who are on your network are who they say they are. Using your access roster referenced above, go through all settings and see if two-factor authentication is possible. Gmail, Dropbox, and a host of others have 2-factor as an option. If you want to get really sophisticated, you can equip your machines with a fingerprint scanner or 2-factor authentication system of its own. Ensure 2FA is turned on for as many applications and trading platforms as possible, evaluate the gaps, and execute accordingly. Also, keep in mind that not all 2FA systems are created equal, SMS, in particular, should be avoided if TOTP or HOTP are available (e.g., Google Authenticator)
7. Tailor authentication according to risk. This is somewhat of a no-brainer, but more rigorous security should be applied to more sensitive activities. Thankfully, most of this will be forced upon the Advisor and is in practice currently (e.g., most custodians require 2 factor authentication of some sort prior to accessing their trading platform). As mentioned above, access to sensitive data (e.g., client files) or high dollar impact operations (e.g., trading) should be targeted.

II. Awareness and Training

In my view, training is the toughest part of being a compliance officer. Team members generally hate it, you lose their attention span after five minutes, and ever Examiner that has walked through our doors has asked: "Can you share your training materials and attendance roster?" Anything you can do to make training interesting, engaging, and effective is needed. Most importantly…

Wesleyina Grayovitch enjoying her annual cybersecurity training.

> With cybersecurity, your closest colleagues can be your worst enemy when it comes to cybersecurity. Write and conduct your training accordingly.

Here are the training basics that all cybersecurity programs need:

1. Schedule cybersecurity training annually at a minimum. Document attendance and ensure all employees get trained (e.g., if someone can't attend, get them trained later on).
2. Highlight key roles and responsibilities. If you have access to everything at the firm, you should probably be aware of the responsibilities associated with that access. Be sure you cover what different access levels mean, particularly for senior leadership.
3. If applicable, ensure third-party vendors are aware of their roles and responsibilities. For most advisors, this does not apply as our third-party vendors probably won't return our phone calls (Google, Amazon). That said, if you have a small vendor providing a bespoke solution for your firm, they need to be looped in on their responsibilities vis-a-vis your firm.
4. WRITE YOUR OWN TRAINING. All firms are different. If you base your training on the key risks identified in your risk management program, then you have a training regimen that actually targets what you need. Off-the-shelf training programs are great to reference but don't rely on them to fulfill what you need. Be proactive and write a program that works for you.
5. Document your changes every year. Create a paper trail of continuous improvement. Regulators want to see an ongoing trajectory of getting better. They are smart enough to separate a "check the box" PDF that gets flashed on a screen once a year versus a bespoke training program.

In my view, this section is the most important. I believe a firm is more likely to be attacked

because of employee oversight rather than some large, anonymous nation-state actor (my hunch is that Iranians and North Koreans are more interested in attacking banks and brokerage firms). Your employees can easily devastate any cybersecurity program by failing to update their machines with patches, running malware detection programs, encrypting their data, etc. With cybersecurity, your closest colleagues can be your worst enemy when it comes to cybersecurity. Write and conduct your training accordingly.

III. Data Security

OK — we are going to get a bit wonky here, but nothing a card-carrying Series 65 license holder can't handle! The main goal of this section is to ensure your data is protected. The best way to protect your data is… drumroll please…encryption and oversight. I will be posting a monster piece on encryption at a later date, but here are the basics.


A WWII era Enigma encryption device. Built by Ze
Germans. Cracked by the Brits.

> Data encryption is where you transform data in such a way that only people with access to a "secret password" can read the data. Going back to our "brilliance in the basics" mantra, you can also regularly review your data to verify you actually need what you are saving. Combining encryption with a common sense data retention policy is a great start to a robust program.

Here are the highlights:

1. Data "at rest" is protected. This requirement means all data on your local machines is encrypted. Some operating systems have full disk encryption tools built in. All you have to do is turn them on. Here is the guide for BitLocker (Windows 10 Pro and Enterprise). There are also an array of encryption tools you can download, many of them free (like VeraCrypt) that will also get the job done. This step is a bit tech-intensive, so be sure to read the full instruction manual first. Also, encrypting your entire hard drive is time-consuming, so I would fire up an encryption process on a Friday night and check on Saturday morning. **Be sure to save your backup codes because your data will be irretrievable if you forget your password and can't find your backup keys. This is by design, if there was a way for you to get your data back without backup codes or you password then a criminal could do the same!**
2. Data "in transit" is protected. This requirement means all of your data that you are

transmitting elsewhere (e.g., trade orders, emails to clients, etc.) are encrypted as well. This step is largely done automatically for most major vendors. Gmail, Amazon hosting, most custodians, etc, encrypt automatically OR you can configure your settings to encrypt (here are the instructions for encrypting Outlook messages). Using this approach, you have to ensure every connection is secure. Not great, but better than nothing. Specifically, you have to ensure every connection is secure when you go online (e.g., the little padlock in the top left corner of your browser is "locked"). Now, if you want to get to best-in-class, a Virtual Private Network (VPN) is the way to go. VPN establishes a "private network" over public ones. When you are at Starbucks and need to crank on some work, the VPN is a sure-fire way to ensure your connection is truly private. You will also get a taste of how people in China get to watch uncensored Netflix. Freedom!

3. Adequate capacity to ensure the availability of data. Unless you are hosting a giant website with tools, blogs, etc., your routine internet connection should suffice. An annual check with your internet provider is likely overkill but certainly checks the box.
4. Protections against data leaks. This action item is closely linked to employee access. Data leaks are best described as data getting out of the company in an "authorized" but unintended fashion. For example, a former employee that never had their credentials pulled is a great example of a data leak (technically, they still had the authorization to access your data). To prevent data leakage, ensure your manual addresses revocation of credentials, working from home policy, and mandatory hardware / mobile configurations (e.g., your screen should lock after so many minutes, mandatory password levels to unlock screens, etc.).

IV. Information Protection and Processes

Sounds complex, but this concept is pretty simple. The main goal here is to ensure systems are set up to protect your data. A lot of overlap with other sections, so I will push through these pretty quickly.

1. Baseline configuration of systems. Simply put, don't just buy a new computer and throw it on your network. Have a new equipment checklist that ensures your computers aren't activated until they are "cybersecurity approved" with encryption, passwords, etc.

Ogadai Khan, Second Khan of the Mongol Empire, conqueror of the Jin Dynasty, and Cybersecurity Overlord of All that is Living, pictured here during an annual cybersecurity training module given to Mongolian forces (c. 1231 AD).

Same goes for mobile.

2. System life-cycle in place. For advisors, another simple task: make sure your systems are updated as they age. A great example is discontinuing Windows versions that are no longer supported with patches and updates. If you are using a platform that is no longer getting patched as vulnerabilities present themselves, it's probably not a good idea.

3. Configuration change processes in place. Another no-brainer. Set up an "admin" password for your computers and ensure only the "admin" can make changes to your machines (e.g., installing new software requires an admin password. Changing screen lock settings requires an admin, etc.). Fairly common sense, low-tech here.
4. Backups of information are maintained and tested. In your compliance manual, ensure your backup systems (e.g., Dropbox, Google Drive, whatever, are working) and test them. Document these tests via your compliance tracker. A great way to test your data is to periodically spot check your files. You can also run a full system restore from your cloud provider, etc.
5. Data destruction. Have a process for purging data. For example, if you have a lot of old statements that exceed the SEC record retention requirements, it might be a good opportunity to routinely purge those files. Should you get hacked, having a client's lifetime of investing activity isn't necessarily a good thing to have stolen. Again, common sense prevails here.
6. Ongoing improvements for data protection. More low hanging fruit. Make this a standard bullet in your annual "cybersecurity review" meeting. Identify room for improvement that is specific to your firm and implement it. Easy day.
7. Sharing lessons learned. As your program matures, reach out to other advisors and share best practices. Hell, go nuts and write a 40-page blog post about it (har, har…)
8. Response and recovery plans. This is a hard requirement that requires particular attention. Ensure your cybersecurity policy has a cybersecurity attack plan and recovery plan. Specifically, if you get hacked, what will you do? How do you maintain service? Write out the steps and sanity check. At a minimum, you should alert the CCO / CTO, disconnect from the network, activate backup files from a backup resource,

assess damage, and confirm with Counsel the notification steps necessary, by state, if sensitive client data was taken or compromised.

9. Test your plans. Do a “sandtable” exercise of #8 above. Walk through what you would do and try to poke holes in your plan. Conduct this activity annually. Bonus points if you do a dress rehearsal and simulate a breach.
10. Incorporate cybersecurity into human resources practices. The easiest way to do this is to add a few “cyber” steps to your existing new employee checklist. Don’t have a new employee checklist? Congrats! You get to write one of those too. A few example steps would be:
    1. Determine access and credentials required.
    2. Receive sign off from CCO / CTO on credentials.
    3. Provide cybersecurity training to new employees and affirm adherence to cybersecurity compliance manual, etc. Again, the common theme here is that every firm is different and you will need to think through what steps make the most sense.
    4. Confirm hardware and mobile device are cyber approved.
    5. Receive final sign off from CCO that employee is “cyber certified” for the year.

V. Maintenance

Maintain your assets in such a manner that prevents outsiders from tinkering with your hardware and software. Two simple points to incorporate into your regimen.

1. Ensure maintenance and repair are controlled. For advisors, this should be simple. Have a simple maintenance request form/log that tracks when computers need repair. Document. Done. The goal here is to prevent individuals from getting their equipment fixed by anyone.
2. Remote maintenance (e.g., remote desktop) is controlled. We touched on this earlier, but have robust controls in place for remote desktop applications (if you even need it). This is a very simple way to “hack” into a network. Thus, maintain the correct settings under which remote login can occur, and ensure an immutable log is kept somewhere. Most importantly, ensure the end user must “consent” to having their machine logged into.

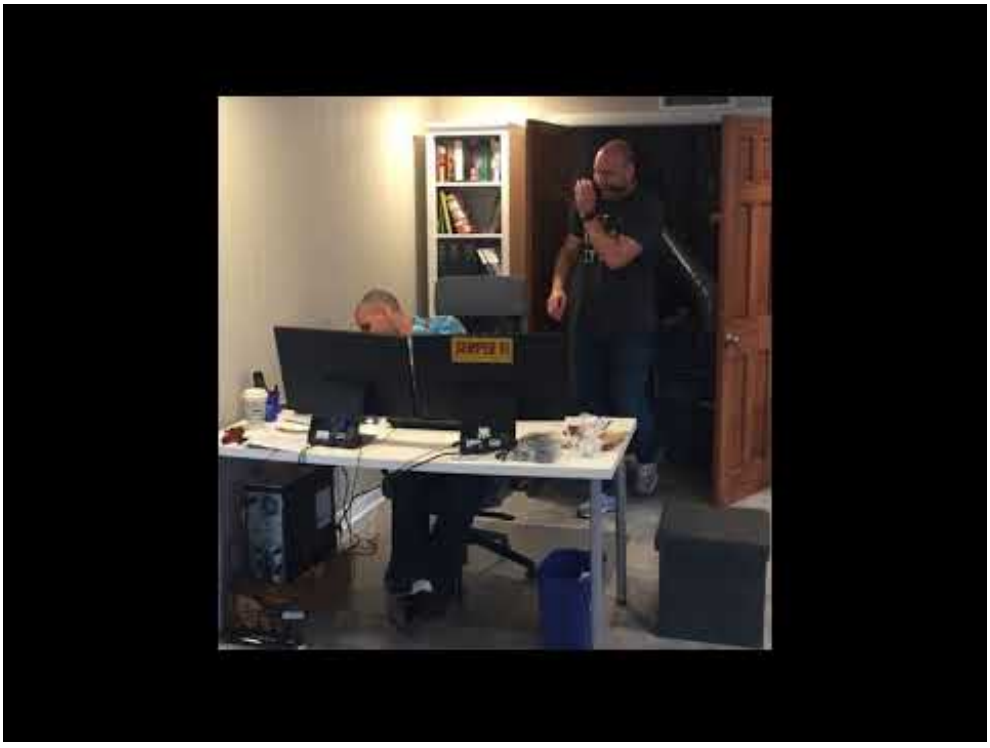
VI. Protective Technology

This section of the NIST framework is brutal, but we translate the basic steps into some key action items below. The core gist of this section is ensuring that any IT settings available can be activated to protect you and your data.

1. Audit/log records are maintained and reviewed. The goal here is to keep a repository of who is accessing your network/data and from where. Granted, most financial

advisors are not going to have the technical know-how to be able to inspect rows upon rows of server data. That said, many third-party vendors maintain access logs that are readily accessible and readable by the layperson. Google Suite, Dropbox, and many others have simple login records and alerts that anyone can download and review. These should be identified and reviewed on a routine basis. Ensure auto alerts are established (typically in the security section of the vendor's admin page) that will notify you of a login from a new computer or location.

2. Removable media is protected. Thumb drives are the devil. That is all I have to say on this topic. Thumb drives are a great way to infect a machine and are incredibly popular with hackers and cybersecurity criminals. Ensure your cybersecurity manual has a clear thumb drive policy. In addition, be sure you disable "autorun" for removable media. Here are disabling instructions for Windows 10. Thumb drives are a great example of the "complacency kills" theme I have been hitting on throughout this post. There is nothing high tech about this measure. It's boring, inconvenient, and will take many "people skills" above and beyond IT know how to cajole your team into true adherence. This is a microcosm of cybersecurity in general. Good processes. Clear manuals. Documentation. Solid training.



https://youtu.be/XZ8WCERyFDc

3. System configured to least functionality. Thankfully, RIA shops are relatively simple operations (as compared to an auto manufacturer or power plant). This principle dovetails with the employee access requirement mentioned earlier – ensure your people have the tools they need to perform their specific role…and nothing more. To the extent you can configure your machines and mobile devices to reinforce this

concept, I recommend you do so. At a basic level, having an "admin" account on each machine that determines password settings, screen locks, etc. is a good start. For data, the more you can segment and cordon off key files, the better.

4. Communications and control networks are protected. A few simple steps to ensure you are current here. First, ensure you have a robust network password, ideally separate from a guest network, in place. This password should be a monster (16+ characters) and very random. Newer routers come pre-configured with tighter security settings than their older counterparts. If you have a network router that is 4 years or older, it might be a good time to get a new one. Also, ensure your router is configured appropriately. Here is a good summary of simple steps you can take to ensure your new router is configured appropriately.
5. Mechanisms are in place to maintain operations in "adverse situations." Some basics here that should be obvious. Antivirus and anti-malware protection should be on and updated at all times. Ensure that all machines are automatically installing operating system updates. If you run a website, it might be worth exploring a cloud-based security application for your web traffic. Cloudflare is a third party vendor that helps prevent Distributed Denial of Service attacks (DDOS). It's easy, inexpensive and anyone can set it up.

Pillar III: Detect (know when you are being attacked).

Now we have a good plan (Pillar I: Identify) and a robust defense in depth (Pillar II: Protect). Now it's time to deploy some commonsense tools to identify where our advisory can expect to be attacked. Thankfully, you are on the downhill slope in terms of NIST requirements. Many of these items are addressed previously.

Thumb drives. The kryptonite of any small firm cybersecurity program.

There are three areas of the "Detect" pillar. I will deviate from the NIST language here to make translation a little smoother. Prioritize your efforts in three parts:

1. Network awareness
2. Continuous monitoring
3. Detection processes

Keep in mind, NIST wrote these sections for all industries and firms, with a focus on firms that can monitor and assess their own threat metrics with a dedicated IT department. As Advisors, we outsource most of this, and we aren't PhDs in Computer Science. So, you get

the watered down version. Of course, extra credit if you go above and beyond the recommendations outlined here.

I. Network awareness

Similar to our first pillar (Identify), we want to focus on identifying the efficacy of our detection system. Where do we want to look and what do we want to find when it comes to network protection. A few simple steps below.

1. Network map. Draw a map of your network and refresh it annually. I know this may sound silly, but there is a method to the madness. Drawing a network map actually forces you to sit down and think about what your network actually is. You may find out that a home office computer isn't included (but should be) or you forgot a vendor that needs to be included in your risk assessment. Speaking of risk assessment, include this network map as an appendix of your annual risk assessment. Now, the shortcomings you find in your map are directly tied to your risk assessment and addressed in your action plan section of the FINRA Small Firm Cybersecurity Checklist! All aboard the Badass Cybersecurity Express. Destination: Your Office. This puppy is starting to pop!
2. Network alerts. Unless you are a computer whiz already, I am going to go out on a limb and assume you don't know how to audit network logs for unauthorized activity. It's a stretch, but let's just assume. For Advisors, I would recommend going through all third-party vendor tools and ensure alerts are "turned on" for logins from new locations, new users, change of passwords, etc. Anything that indicates new activity should have an alert sent to an admin user. The main goal here is to establish the "trip flares" on your network to be aware when someone is accessing your network.

II. Continuous monitoring

Take the network alerts you have established and document in your cybersecurity manual who needs to audit, review, refresh, etc. and how often. For example, a quarterly refresh of all network alerts for Gmail, Dropbox, and your custodian is a good process, at a minimum.

Some additional tips below:

1. Monitor both the physical environment and personnel activity on the network. You have the perimeter, now post the alerts to watch it….
2. Detect malicious code. Sounds complex, but have the necessary anti-malware, virus protection on autopilot (and regular checks) will ensure you have a good system in place.
3. Monitor external service providers…this is a tough one for the reasons outlined above. That said, routine checks on key service providers (even documenting a quarterly check in at a minimum) are a good start.

4. Monitor for unauthorized users, devices, and software. This step is already covered in prior sections. If you are doing well there, you are doing well here.
5. Vulnerability scans in place. Very close to #2 above. Maintaining ongoing anti-malware / antivirus should suffice for most.

III. Detection Processes

A very common sense section. Let's attack these quickly:

1. Clear roles and responsibilities for detection. Basically, put what we just discussed above in a compliance manual, designate owners, and identify a process.
2. Detection activities are tested. Very simple. If you want to be alerted when X, Y, or Z happens on your network (Gmail login, etc.), test the alerts to ensure they are on and functioning as you want them to be.
3. Detection events are communicated. The easiest way to accomplish this is to send all alerts to a shared listserve "alerts@acmeadvisory" to ensure the right people see alerts as they happen.
4. Continuous improvement. Take all that we have discussed in this pillar. Talk about it during your annual review. Figure out ways to make it better. Document. Improve. Wash. Rinse. Repeat.

Again, some IT-specific activities here, but lion's share of this pillar is documenting your process, ensuring people own and improve it, etc. You can do this.

Pillar IV and V: Respond and Recover (doing the right thing in the event of an attack).

A good response plan is critical for any cybersecurity program. All advisors should have a plan for what happens in the event of an attack. I recommend including this plan in your "Business Continuity Plan" that all advisors should have OR writing a cybersecurity response plan as a separate section.

Beehive Station #6578-B deploying their Response and Recovery plan against Todd the Beekeeper.

Note*: we are going to combine these sections into one as the topics are quite similar. Almost*

there team*, I can see the barn…*

There are four key areas within “Respond and Recover”:

1. Response and Recovery Planning
2. Response and Recovery Communications
3. Analysis and Mitigation
4. Improvements

Most advisors will be relying heavily on their third-party vendors (e.g., Google, TD Ameritrade, etc.) in the event of an attack. That is 100% acceptable. So long as your plan is documented, well thought out, and regularly reviewed/improved, you should be okay.

I. Response and recovery planning

Very simple here. Plan in writing. Plan rehearsed. Key owners understand. Training incorporated. I won’t even torture you with sub-bullets on this one.

II. Response and recovery communications

Also straightforward, but some nuance that all advisors should be aware of:

1. Clear roles and responsibilities. Who handles the internal execution of the plan? Who talks to clients? Who notifies regulators?
2. Notification criteria. What will trigger our plan? Who has the authority to trigger our plan?
3. Coordination with stakeholders. How will we engage our service providers if we think there is a breach?
4. Voluntary information sharing. Somewhat difficult for smaller shops, but sharing lessons learned with the broader advisory community is always worthwhile.
5. Public relations. Let’s spend some time on this one. There are state-by-state notification requirements if, in fact, you are hacked or your data is truly compromised. Any RIA Counsel worth their salt should have the notification requirements, by state, that apply. Your clients in California will probably have different requirements than your clients in Delaware, etc. Now would be a good time to find a decent attorney that you can have on standby if, in fact, your data is stolen.

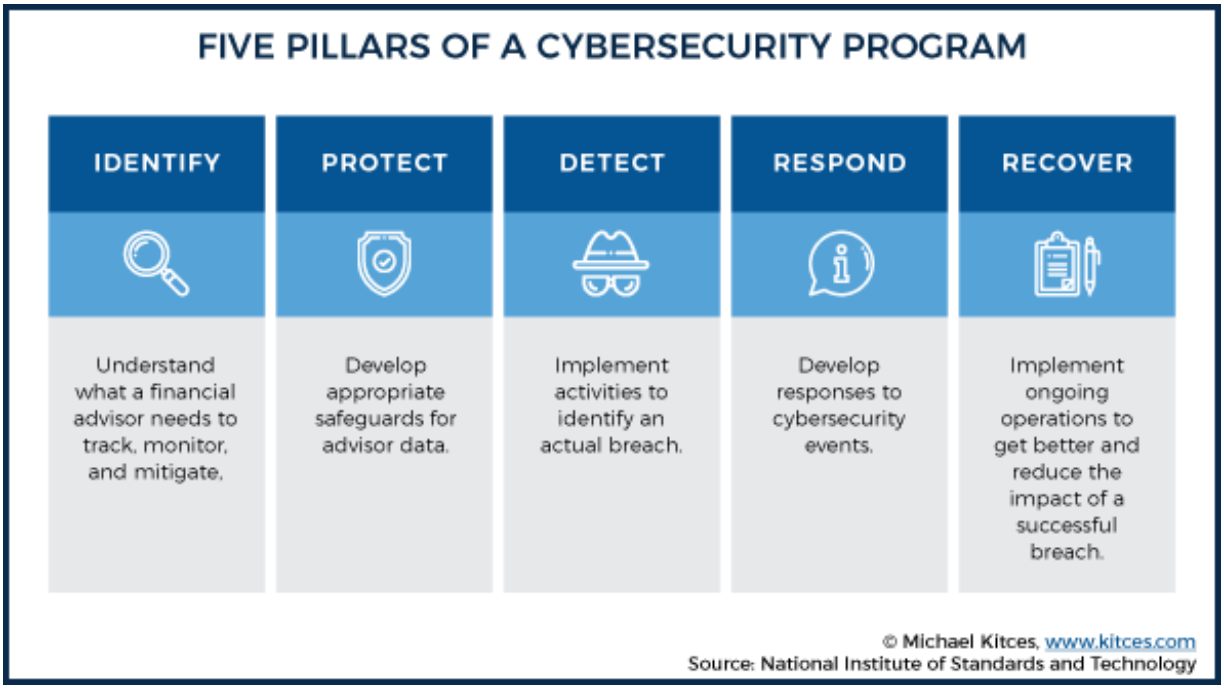
III. Analysis

Most advisors probably lack the technical know how to effectively diagnose a cybersecurity attack. Your best bet is to maintain a strong offense (described above) and ensure your network alerts are active, current, and configured properly. For larger firms, it may not hurt

to retain a third party service provider to test and analyze your defenses in place (see my post here on penetration testing). In the event of a breach, knowing how to quickly isolate an attack (e.g., go offline, disable a user, etc.) can go a long way.

IV. Improvements

I can't stress this enough. Regulators want to understand the evolution of your program. They want a timeline of enhancements, not a still-frame photo of your current program. Many aspects of this will seem foreign or intimidating. Brush those worries aside, put pen to paper, and get something on the tape. Demonstrating effort and taking the first step is essential to building a program.



Conclusion: Cybersecurity is Tough but Doable.

Kudos if you made it this far! A quick recap for achieving SEC cybersecurity compliance:

1. Get smart on the SEC website to get the lay of the land (see the top of the post).
2. Get the NIST framework and read it.
3. Export the NIST Excel framework.
4. Write your compliance manual using the Excel matrix.
5. Update and improve.

A lot to consider, but doable. Your clients and your practice will be better for it and you will meet any exam with a good program.

Of course, we are always looking for better ideas and recommendations. Feel free to email us with what you are seeing and learning.

And remember…

Complacency Kills!

SEC Cybersecurity Requirements for Registered Investment Advisors (RIAs) was originally published at https://alphaarchitect.com/. Please read the Alpha Architect disclosures at your convenience.