Chapter Nineteen

Hacked!

*If you spend more on coffee than on IT security, you will be hacked.”*

–[Richard Clarke](https://thehabitstacker.com/cyber-security-quotes-that-will-blow-your-mind/)



Bernadette wasn’t looking for information about cybersecurity problems per se, but the information jumped out at her while she was perusing the Internet, preparing for her next meeting at Elaina’s house. The first article that caught her eye was a Securities and Exchange Commission (SEC) document that outlined a worrisome trend about financial advisors who were not in compliance with recent laws.

In 2024, the SEC issued the results by their examination staff, which found RIA and brokerage deficiencies in safeguarding customer records and information at branch offices. Eight financial planning firms were named by the SEC for lackluster cybersecurity policies that led to ‘email account takeovers exposing the personal information of thousands of customers and clients at each firm.’

According to an SEC claim, all the firms were Commission-registered as broker-dealers, investment advisory firms, or both. The SEC levied a $300,000 penalty for their lax behavior. Because of this, the SEC said that from November 2017 to June 2020, email accounts at sixty financial firms were hacked into, leading to over four thousand customers and clients having their personal information leaked.

The SEC’s order also found that each of the firms claimed to have sent breach notifications to their clients, which included misleading language suggesting that the notifications were issued much sooner than they actually were after discovering the incidents, according to the SEC statement.

This was a public warning to all financial advisors. RIAs must update their policies with any new rules for compliance and revisit any specific policies created by the firm to improve internal processes. This includes a system for backup because outdated backup drives can cause many issues if they are not compatible with company systems.

This hadn’t even occurred to me, Bernadette thought. Is Blackburn Financial in compliance? Does he have the right protection for his clients? Is it possible that my home computer provides me with more security? Depends on how careful Sandy is, she concluded. But then, worry set in. This can’t wait until our next meeting.

“Janie, do you have a minute? You’re the tech expert between the three of us. Do you know how well Sandy’s office protects our financial records from hacking?”

“I never thought about it, Bernadette,” said Janie. “Why the sudden concern?”

“I was getting ready for our meeting on Saturday when found an article on the SEC’s website. They issued a warning to all financial advisors reminding them that they are required to have policies and protections in place regarding cybersecurity, or they can expect to face sanctions.”

“If it’s that widespread of a problem, then the three of us need to discuss it. My health insurer got hacked last year. I opted for their free offer of protection through one of the credit bureaus. The hackers got everything, including my social security number. To make matters worse, my health insurance company waited six months before they sent out the notice. I change all of my passwords regularly now, and I placed a credit freeze on all three of my credit reports.”

“I’d like some written information from Sandy about what he’s doing to protect our information. I’ve been reading about sloppy dealings at big firms. Some of the largest firms in the country have been fined millions for not complying and not keeping up to date.”

“Can you tell me anything specific?” asked Janie.

“One firm failed not only failed to prevent the hacking, but didn’t shut down their operation adequately once they were alerted that the breach had happened. The SEC fined the company under the Identity Theft Red Flags rule. Cybercriminals posed as advisors and asked for and received usernames and passwords from the company’s support personnel, ruining the accounts of 5,600 customers. The SEC concluded that the breach occurred in part because its personnel didn’t have a full understanding of how its own portal worked.”

“And this is a big firm,” said Janie. “I’ll bet the smaller firms don’t have the time or resources to devote to shielding themselves from a big attack.”

“You got it, Janie. I read another article referring to small firms as low-hanging fruit. State-registered small firms, like Sandy’s, showed more deficiencies. Their cybersecurity deficiencies included inadequate insurance, lack of vulnerability testing and weak or infrequently changed passwords.”

“I wonder what low-hanging fruit means exactly,” said Janie.

“In numbers, it means there’s eighteen thousand state-registered investment advisers that are one or two-person shops. And the state regulators expect these crimes to be on the rise. The good news in the article was that many advisers were reportedly stepping up their compliance efforts.”

“I think the three of us should talk every week about scams that we read about. I love reading through these stories, and I think they’re fascinating. Maybe it’ll help us to stay on our toes,” said Janie.

“I’ll keep reading,” said Bernadette. “Elaina is too busy with her mom right now. We’ll surprise her on Saturday with these extra nuggets of information. This is one more thing to add to our list of questions for Sandy.”

\*\*\*

Sandy was the type of guy who liked to be on the move. Sitting still was not his forte. He loved chatting people up, making sales, and handling money. Mostly other people’s money. He understood that the world of cybersecurity was a rapidly evolving safety issue, however, a full understanding of the current laws had evaded him. Sandy had decided that either his quick texts and trades were too infrequent to worry about, or that he was well under the radar for any criminals to take an interest in. Perhaps Sandy had a touch of attention deficit disorder himself. Whatever one might speculate about his reasoning behind his choices, Sandy was making mistakes and in clear violation of FINRA rules. Being out and about with cell phone in hand was the perfect combination for Sandy to make snap decisions and fast trades.

The SEC and FINRA don’t prohibit the use of personal email accounts or text messaging – referred to as “off-channel” communications. But their laws and rules require firms to preserve records related to their business. This includes the review of incoming and outgoing communications with customers, including electronic communication such as texts.

If only Sandy had been attending ongoing continuing education as required, he would likely have taken the necessary steps to reinforce his records and, therefore, his security. But Sandy had obtained no education credits in the past year and had been letting things slide.

During the past few days, Sandy had received high usage notifications from his cell phone carrier. He hadn’t changed any of his usage patterns. In fact, he’d probably used his phone less. His battery was draining faster, and he was getting bombarded with pop-ups.

Ben received a notice from his bank confirming a large withdrawal, which he had not made. “Elaina, did you make a three-thousand dollar purchase today?”

“Of course not, Ben. Why do you ask?”

“I just got a message from the bank about a withdrawal. Can you call them and see what’s going on?”

Elaina took immediate action. Instead of calling them, she made the five-minute drive to the bank. “Hello, Mrs. McNamara, what can I do for you?”

“My husband just phoned me about a withdrawal from the bank for three thousand dollars. Neither of us made any purchases in this amount.”

“Have a seat and let’s see what’s going on,” said Susan, the bank’s representative. “It looks like the withdrawal has something to do with your financial or brokerage account. Do you have a financial advisor who trades on your behalf?”

“We have a financial advisor. His name is Sandy Blackburn, but he’s not allowed to make any decisions or trades without contacting Ben or I first.”

“I recommend you start him. If he didn’t initiate any financial charges, then perhaps there’s a problem at his firm. I think you should stay here and try to reach him now. Put us on speakerphone. If he’s aware of what happened, I’d like to hear his explanation. That way, I can help to mitigate your losses.”

“Sandy, this is Elaina. We’ve got a problem. Three-thousand dollars has just disappeared from our bank account, and the bank representative asked me if I had any information about the purchase of stocks or mutual funds. She’s on speakerphone with me now. Did you make any trades that might have affected our bank accounts?”

“No, Elaina, I don’t have access. I would never do that.”

“Mr. Blackburn, this is Susan from First National Bank. Is it possible that you made trades recently from your cell phone? Hackers often gain access to client’s financial information when financial advisors trade from their personal cell phones.”

Sandy fell silent. This could explain the irritating issues he’d noticed on his cell phone lately. He had, in fact, been hacked. “Elaina, someone may have hacked my phone. I made a few trades for my clients while I was on the road a couple of weeks ago. I’ve been getting a lot of pop-ups, my battery charge has been getting depleted quickly, and I’m getting a lot of unwanted calls.”

“Thank you, Mr. Blackburn. I’ll move forward as if there’s been a crime committed and I’ll advise Mrs. McNamara about steps she can take to stop further problems. To begin with, I’ll place a stop order on her bank account until we can implement changes. Will you be reporting this to your regulatory authorities?”

“Uh, no, I don’t think that’s necessary. I’ll change my passwords.”

“What about my three grand?” screamed Elaina.

“Mr. Blackburn, do you have a Written Information Security Plan in place?”

“No, not yet. I’m working on it.”

“What’s entailed in this kind of plan?” asked Elaina.

“A WISP, as it’s referred to,” said Susan, “Is a plan that should state in detail appropriate administrative, technical and physical safeguards to protect your client’s private information. A main point is that all devices containing any private information are required to be encrypted. That prevents unauthorized parties from seeing private information.”

“You’ve never told Ben or I about how safe our information is, Sandy,” said Elaina. “Now that I think about it, the last email you sent didn’t have a secure encryption notation on it. In the event of a theft, Sandy, do you have any insurance to cover our loss?”

“I have insurance. I’ll check my policy as soon as I get back to the office and call you back.”

“Thanks Sandy. Call me back as soon as you can.”

As Elaina ended the call, Susan was staring back at her. “Elaina, in order to make your claim have as much teeth to it as possible, I think we should alert FINRA. They oversee problems like this, and it sounds like your financial planner may have been a bit lax in implementing protections for his clients. If we report him to FINRA, it’ll strengthen your case.”

“I don’t have any problem with that. What else can I do?”

“Mr. Blackburn is obligated to provide you with a written plan that outlines in detail the safeguards he has in place. If he doesn’t have such a document, he’s in violation not only of FINRA’s rules but SEC laws. It’s all a part of maintaining proper records and that includes texting and emails. The SEC takes this kind of thing very seriously. They recently fined eleven different firms for a combined two-hundred and eighty-nine million dollars.”

“I can’t believe it.”

“To start with, I recommend you go home and change all of your passwords and pins on all of your accounts. That’ll help to prevent fraudulent access to these accounts. I also think you should check all three of your credit reports. If you haven’t reviewed any of your credit reports in the past twelve months, you can access them for free by going to <www.annualcreditreport.com>. You should also contact all of your credit card companies and any other banks you work with.”

Elaina wrote all the recommendations down as fast as she could. “This is the last thing we need. My mother is in hospice. I’ve been sick and out of work, and now Ben will panic.”

“No need to panic,” said Susan. “Treat this like getting into a car accident. By that, I mean, get a copy of your advisor’s insurance cybersecurity information.”

“I hope he has coverage.”

“Elaina, without proper cyber insurance and an incidence response plan, your advisor’s practice more than likely will not survive the breach. Now, let’s notify FINRA.”

\*\*\*

Once Sandy returned to his office, he found five voicemails and three emails from more clients, all alluding to the same concern. Quickly sifting through his policy, he could ascertain that, depending on the losses, he had a reasonable amount of coverage.

After returning numerous phone calls, and barely succeeding at assuaging his client’s outrage, Sandy went to work on developing a document that detailed his procedures to prevent hacking. That involved extra software and encryption. Better still, Sandy needed to increase his coverage.

While at his desk, he took one last phone call. It was from Ben McNamara. “Hi Ben. I’ve been working on your account, and I’m making a claim to help you recover your money. My cell phone has been hacked, and the hackers were able to obtain your personal and account information. I’m sorry. I’ll make this right.”

“This has turned our lives upside-down, Sandy. Elaina and I are up to our eyeballs in stress. I’m working sixty-hour weeks to keep the household going. This is not okay.”

“I know, I know, and I feel terrible. I’m scrambling right now. This has happened to more of my clients, too.”

“What? Well, I wanted you to hear this directly from me. On the advice of our bank, we’ve reported this incident to FINRA. They may well report you to the SEC, too. Don’t be surprised if you hear from one or both of these agencies.”

“It’ll be ok. I’ve been making changes to insure everyone’s security right now. I’ve notified my insurer and we’ll work this out.”

“On that note, we want a copy of your insurance coverage. I don’t have time tonight to get it, and I don’t want you to send it by email. I’ll be over first thing tomorrow to pick it up. I’m not finished talking with you about this, Sandy. I want details about how this happened.”

“I’ll have it ready for you.” Sandy wasn’t completely clueless about the rules and laws pertaining to protecting personal data. He, too, had read an article about financial advisors who’d misused texts and emails so they could make exaggerated claims about returns, performance guarantees, pressure to decide quickly about an investment, or other content inconsistent with federal securities laws and FINRA rules. Sandy was up to the very same deception and did so in order to circumvent audits by any authority because making false claims was also a definite violation of federal securities laws.