ARE YOU EXPOSING YOUR CLIENTS, THEIR MONEY, AND YOUR PROFITS TO CYBERCRIME?

Why You Should Take
Cybersecurity Personally

By John Sileo
ARE YOU EXPOSING YOUR CLIENTS, THEIR MONEY, AND YOUR PROFITS TO CYBERCRIME?

Why You Should Take Cybersecurity Personally

By John Sileo

If someone walked up to you on the street and asked for your client’s Social Security number, would you give it to them? How about the keys to the net worth of all your clients combined?

If your answer is no—you would never knowingly expose your client’s personally identifying information—then you would be wise to take a close look at your current cybersecurity practices.

From my experience peering inside hundreds of financial advisors’ practices, many are lacking up-to-date cybersecurity controls and some already have put their advisees’ bank and investment accounts in jeopardy.

To determine if your cyber strategy falls short, ask yourself or your technical team if any of these key risk indicators apply:

- It has been more than a year since your last comprehensive external security penetration test.
- You don’t know what a security penetration test is, why it has to be external, or have never had one performed.
- You don’t have a separate technology budget for security controls and maintenance.
- You wouldn’t be 100-percent prepared to restore backups of key files and systems from scratch within 24 hours if your data was locked up by cybercriminals for ransom.
- You haven’t prepared a breach response plan that spells out who will deal with the public relations nightmare of a breach, how you will communicate with affected clients (to minimize legal liability), who will make up the post-incident response team to manage damage control, and how this team will organize when all systems are down.

The reality is that you and your clients probably already have been compromised in some way, and the financial consequences could be substantial. According to a 2018 study conducted by the Ponemon Institute: “Organizations that lost less than one percent of their customers due to a data breach resulted in an average total cost of $2.8 million. If four percent or more was lost, the average total cost was $6 million, a difference of $3.2 million.”

When I gave my cybersecurity keynote speech at the Investments & Wealth Institute Annual Conference Experience in May 2019, I asked audience members to stand if they’d ever had a credit card number stolen or information compromised in a data breach, and 90 percent of the audience stood. Those are staggering figures. But statistics don’t begin to capture the human toll that cybercrime takes on its victims. I know because I was one of them.

CYBERSECURITY ISN’T JUST ABOUT DATA—IT’S ABOUT LIVES

I didn’t take the easiest path into fighting cybercrime. In fact, I’m a two-time victim. The first time, my Social Security number was stolen out of my trash, sold on the dark web, and used by a woman to buy a home across the country. I found out one day when I walked into my bank and, in addition to learning that my family’s life savings was gone, was escorted out by security guards for crimes the identity thief committed. It didn’t matter one bit online that my thief—a woman—was posing as a man.

When a special agent from the district attorney’s (DA) office showed up at my door, I assumed it was to give me good news about capturing the criminal and returning our money. Instead, the agent handed me a subpoena and said I was going to jail.

In a voice so calm it was menacing, the DA told me I was going to be charged for electronically embezzling $298,000 from my customers. He said the DA’s office had enough digital DNA to put me in jail for a decade. And then he left me on that doorstep, shaking in front of my two daughters. Fast forward two years through my criminal trial, fighting every day to keep myself out of jail for crimes I had nothing to do with. I lost my $2-million software company, my family business, and most importantly, more than two years of paying attention to my family.
I share the full story during my speeches, and I won’t spoil the ending, but needless to say I have a very personal reason to care deeply about cybersecurity. I still get emotional when I think of my five-year-old daughter asking me why I had stopped paying attention to her. It took every moment of my time to keep myself out of jail and try to rebuild my small business.

I honestly didn’t think our little company was big enough for a cybercriminal to bother with. But I was naive. In 2018, 58 percent of data breaches were at small businesses, and 28 percent of data breaches involved internal actors. It’s less surprising that 76 percent of breaches were financially motivated. It takes an average of 73 days for organizations to contain an insider-related incident; in my case, it took much longer.

What’s most important to you? Time with your kids? Your home? Your wealth? Your business? Because that’s what you risk losing if you fail to act. The harsh reality is, in an information economy, it’s no longer just about the security of data. It’s about the security of everything.

**PUT ON YOUR OWN OXYGEN MASK FIRST**
The 2018 Verizon Data Breach Investigations Report found more than 53,000 incidents and 2,216 confirmed data breaches. In 2018, there were 134 data breaches in the banking, credit, and financial sectors alone, exposing more than 3 million records. This should worry you, and undoubtedly it does. As a professional, you want to keep your clients’ data safe, but you may not be doing everything you can to achieve that goal. Your staff may not be doing everything they can, either. Why? Because it’s not personal.

My experience working with hundreds of clients has demonstrated that knowledge alone doesn’t create change; emotions create change. When your employees make a personal connection to the data and how it impacts the most important aspects of their world, their behavior will change. Until you, your employees, and your coworkers make a personal connection to the data you handle every day, you won’t take true ownership of corporate data. In airline safety parlance, you need to put on your oxygen mask first.

Most organizations skip the step of making security personal for their people before they ask them to protect the corporate data. A culture of security grows out of every employee and executive understanding why they need to protect their own data before they’re asked to protect someone else’s. Make protecting your clients’ data as automatic as breathing.

A strong cybersecurity posture begins with understanding the main threats and their solutions. Here is a brief rundown of each.

**SOCIAL ENGINEERING**
Social engineering is when a hacker manipulates a victim into divulging information (such as a password or Social Security number) or taking action (such as clicking on a link, downloading software, or inserting a thumb drive). Think of those fraudulent calls you get from someone pretending to be from the Internal Revenue Service or phishing emails that purport to be from your bank and ask you to click on a link to update your information before your account is cancelled. These emotion-inducing appeals are the tip of the hacker’s spear. It’s far less costly and time-consuming for criminals to get the information just by asking rather than hacking your systems with brute force.

Social engineers hijack your auto-responder—the reflexive response that occurs before deliberate thinking takes over. They do it with your receptionist and they do it with your information technology person. Criminals always will go for humans first, yet we as businesses tend to fund the training of our humans last. That’s true in every corporation and small business I’ve worked with, especially those that handle as much personally identifying information as financial advisors.

Most social engineering attacks start with the criminal performing reconnaissance on the target using social media profiles and posts. If they know where you were born, your children’s names, your job, and where you vacationed last summer, it’s much easier for them to gain your trust in pursuit of even more valuable information, such as cloud login credentials.

To stop social engineering attacks, you and your people need what I call security reflex training (SRT). Unlike security awareness training, which educates you primarily about the threats that exist, SRT first makes you aware and then teaches you exactly how to respond to requests for information or access. In essence, you’re training your workforce to replace their natural inclination to be kind and helpful with a brief, skeptical pause while they do a bit of critical research. That way, when the criminal sends an email with intimate details of the target’s personal life in an attempt to get them to click on a link, the target knows to slow the process down, think critically, and ask the right person what to do before clicking. Stop. Think. Ask questions. That reflex has got to be automatic.

**KNOWN VULNERABILITIES**
It’s easy to feel overwhelmed and powerless by the number of cybersecurity threats out there, but here’s the good news: 95 percent of them are known vulnerabilities—threats that have been around long enough that we can predict them. And that means they’re solvable. Here are the most common oversights inside small and medium-sized financial practices, as well as in many of your clients’ homes:

**Outdated operating systems.** Windows XP and 2000 still are widely utilized in business, but neither has been supported
by Microsoft for years, making them hackers' easiest back door into your entire network. The same goes for outdated Mac X operating systems.

**Poor security patching.** You might have the latest operating system, phone app, or software package, but that doesn’t mean you have the latest security patches installed. In most cases, setting up automatic software updates will solve the lion’s share of the problem.

**Weak passwords.** Most account and cloud takeover is made possible by bad password habits. Implement password managers to maintain long and strong passwords in your organization. Also, turn on two-factor authentication on all critical accounts.

**Spotty encryption.** In your industry, data encryption is fairly heavily mandated, and yet we see numerous examples of firms failing to implement strong encryption across their systems.

My recommendation is that you hire a reputable security firm to configure your encryption and assist with the other items above. Just as your clients can’t manage their wealth without the skill and experience you bring, you can’t manage your data security as well as someone who does it professionally.

**SPEAR PHISHING**

Phishing is where the criminal sends you an email or text with an enticing link that’s been socially engineered to get you to click. When you take the bait, they download malware onto your system or upload your login credentials to their well-protected servers. Spear phishing is simply a more sophisticated form of phishing. The criminal has a little bit of information on the victim, generally from the victim’s social media profiles, and they use that knowledge to gain a foothold. We now have spear phishing enabled by artificial intelligence, where the criminals are using artificial intelligence to mine, for example, the Facebook profile of you and every one of your connections before sending you the malicious email.

Again, they are building credibility that their request is legitimate, but this time it’s automated by computers, allowing them to gather your buying and browsing habits, friendships, and public posts before they strike. For example, they don’t just know you were affected by the recent Marriott breach, they know the last Marriott hotel you visited, where you went to dinner that night, and what you ate for dinner. When they contact you pretending to be Marriott to say your credit card was declined at that meal and you need to give them a replacement, you’re likely to believe it.

Back in 2015, a systems administrator at a subsidiary of Anthem fell victim to a spear phishing scam, clicked on the link, and exposed 80 million personal records to a cybercriminal in China.7

Here’s an easy way to verify the authenticity of the email: Hover your cursor over the sender’s name. When you hover over marriott.com, the email address will read something like marriott.gibberish.ru. You’re surfing to Russia. Ninety-nine percent of the people inside your organization don’t know this simple tool of detecting phishing, and it’s vital that they learn and implement it.

Additionally, you need to implement gateway-level spam filters to remove as many phishing attempts from your firm’s email system as possible. Technology will help you remove more than 90 percent of the malicious emails; your people need to be trained to catch the other 10 percent.

**WHALING**

Whaling is the big brother of spear phishing. In this case, the criminals go after the top executive: the chief executive officer or chief operations officer. We also call this business email compromise or wire transfer fraud; they’re all cousins.

This is how it works: The cybercriminal fakes an urgent email from a company executive to a subordinate, requesting either sensitive data or a large money transfer. Oftentimes, the scammer sends the email when the executive is out of town (which they learn from social media), so it’s more likely the subordinate will simply follow the instructions.

According to FBI statistics, between October 2013 and May 2018, whaling operations cost businesses worldwide more than $12 billion, but the actual figure is undoubtedly far higher because many companies don’t report the crime. One notable example is Ubiquiti Networks, which was swindled out of $46.7 million in 2015.9

Implement controls that won’t let any one person inside your firm wire transfer large sums of money without a second approval. This will make it much harder for overseas cybercriminals to convince
one poorly trained employee to hand over the keys to the cash register.

**RANSOMWARE**

Ransomware is a kind of malware that locks or denies access to a computer’s files until a ransom is paid. Typically, ransomware is spread through phishing emails, visiting an infected website, or through an external device, such as a thumb drive. Private companies, city governments, and large hospitals have all fallen victim to ransomware attacks. Because so many victims pay the ransom, it’s a lucrative crime and its use is on the rise. In August 2019, it was reported that 23 towns in Texas were hit by a coordinated ransomware attack and earlier this summer the city of Riviera Beach, Florida, paid $600,000 to get its data unlocked. About 50 percent of the time, in my experience, paying the ransom unlocks the files. Half the time, though, victim organizations pay the ransom and still never get their data back.

The best defense against ransomware is a strongly encrypted backup—with two caveats: You have to restore your backup on a regular basis, so you know it works and that it’s restorable (most companies forget this step). Second, it needs to be a 3-2-1 backup. You need to have three separate copies of your data on at least two media types (for instance, one in the cloud and one on tape backup or on a physical hard drive), and one backup should be offline and offsite. You need the backup so you can restore your files over the systems you’ve been locked out of without having to pay the ransom.

Educating your team about the above data security threats—and instituting the respective solutions—could give you the single greatest return on investment of any other investment you make in your company. The Ponemon report found: “Companies that identified a breach in less than 100 days saved more than $1 million as compared to those that took more than 30 days to resolve.”

**LEVERAGING CYBERSECURITY AS A UNIQUE SELLING PROPOSITION**

I give 75 presentations a year. The number one requested topic among financial advisors is how to help clients secure their own data, both from a privacy and security perspective. Your average client doesn’t know how to freeze credit, implement passwords to keep hackers out of their financial accounts, or configure a smartphone to protect mobile banking, investing, and health monitoring.

Educating your clients about these precautions is an effective way to differentiate yourself from your competitors. At the end of the day, you’re not simply managing wealth; you’re managing lives. Your clients trust you more than they trust their bankers, and you want your current and potential clients to understand that you take that responsibility seriously.

Very few firms offer this type of information to their clients and those that do have a competitive advantage. Whether through a client appreciation event or personal consultation, when an advisor helps clients protect their data—thus lowering their risk profiles—it deepens their trust.

Your customers are incredibly worried about these issues. By tightening cybersecurity at your firm and teaching your clients how to protect themselves, you both win.

---

John Sileo is the founder and chief executive officer of The Sileo Group, a cybersecurity think tank, in Lakewood, Colorado. He earned a BS with honors in political science from Harvard University. Contact him at sileo.com.

---

**ENDNOTES**


2. Verizon, “10 Key Takeaways from the 2018 Verizon Data Breach Investigations Report,” (November 12, 2018), https://www.verizondigitalmedia.com/blog/10-takeaways-from-the-2018-verizon-dbi-report?creative=308203995558&keyw...&b=t_308203995558_bk_&bmm=b&bn_...=57195208501&clid=EAalOobcCHMi-deqQBHSIAIGyz5yZh0r0ACKEAYAAIAAAEg.xF_D_BwE&creative=308203995558&keyw...=57195208501&clid=EAalOobcCHMi-deqQBHSIAIGyz5yZh0r0ACKEAYAAIAAEg.xF_D_BwE.

3. Ibid.


5. See endnote 2.


12. See endnote 1.