CYBER-
SECURITY

Cybersecurity: 5 Steps Every Financial Advisor Should Take to Protect Their Practice and Clients

Mike McGlothlin, EVP, Retirement - Ash Brokerage

Andrew Dahman, Chief Technology Officer - Techficient

Dave Barcelona, Chief Information Security Officer - Techficient

ASH BROKERAGE
Ash Answers.

A New Financial Frontier

IN AN EVER-CHANGING WORLD, DIGITAL SECURITY IS A MUST

The last four years have been eventful in financial services. We saw the conclusion of one of the longest and strongest bull markets in recent history. President Trump brought disruption to the political arena while pushing an agenda that lead to the most significant tax reform in several decades. And, geo-political forces increased tensions with North Korea, the Middle East, and even the United States' strongest allies.

All the above make for yet another challenging environment to manage money, plan for retirement incomes, and distribute wealth. With so much noise, it's easy to forget about running a small business and the risks associated with it. Whether you're a standalone Registered Investment Advisor (RIA) or a registered representative with a broker-dealer, there's one factor you can't afford to ignore: cybersecurity.

Digital privacy and security are more important than ever. As Jason Hart, vice president and chief technology officer for data protection at Gemalto said, "Security is no longer a reactive measure but an expectation from companies and consumers."[1] Customers have begun to view the financial services industry's cybersecurity practices as table stakes before engaging with a planning firm.

Unfortunately, many advisors, in general, have not made necessary changes to protect their clients. That opens an opportunity for other advisors to create a value gap between their firm and the competition.

The good news? It's not too late to catch up to best practices. You can not only help protect your own business against cyberattacks, but you can also help educate your clients to avoid fraudulent activity.

> *Security is no longer a reactive measure but an expectation from companies and consumers.*

WHY IS CYBERSECURITY SO IMPORTANT?

Some facts to consider:

- Hackers attack every 39 seconds on average 2,244 times a day[1]
- 53% of companies had over 1,000 sensitive files open to every employee[1]
- 43% of breach victims were small businesses [1]
- 56% of Americans don't know what steps to take in the event of a data breach[1]

Even after being victims of a cyberattack, many business owners aren't properly reinvesting to protect client data. According to a Barkly report, 52 percent of firms that were victimized had no plans to adjust their security plans.[2] And 45 percent of those firms didn't plan to increase their budget for security needs.[2]

We need to help our clients protect themselves as well. We already know the elderly can fall victim to phone or mail scams that fleece many from retirement savings. Cyberattacks are no different. And, because cybersecurity is new to so many, your clients – of all ages, net worth, income levels, and education levels – are susceptible to cybercrimes.

According to an interagency federal report, more than 4,000 ransomware attacks have occurred every day since the beginning of 2016.[3] Even if you think you're protected, human nature makes it easy to become a victim. According to a survey by Friedrich-Alexander University, up to 56 percent of email recipients and around 40 percent of Facebook users clicked on a link from an unknown sender although they knew of the risks of their computer becoming infected with a virus. Why? Curiosity.[4]

every 39 seconds

or

2,244 times per day

hackers attack

53%

of companies had over 1,000 sensitive files open to every employee

43%

of breach victims were small businesses

56%

of Ameicans don't know what steps to take in the event of a data breach

WHAT SHOULD YOU DO TO PROTECT YOUR BUSINESS?

Your clients' financial assets are too important, and the risks are too high for your reputation, your business, your clients and their families, to ignore the threat of a cyberattack. According to the Federal Trade Commission (FTC), there are five simple things you can do to better prepare your business for the increase in cyberattacks going forward.[6]

1. **Take Stock**
2. **Scale Down**
3. **Lock It Down**
4. **Pitch It**
5. **Plan Ahead**

These steps are so simple that every business owner should be implementing them and sharing them with clients. In this white paper, we've summarized the FTC's recommendations and added insights specific to the needs of a financial services firm.

1. Take Stock

It only makes sense to understand where you are today as you develop your cybersecurity plans. Much like any financial planning process, you must take stock of where your clients stand before planning for their future. So, begin by taking inventory of all your "at risk" assets.

- Make a list of all your computers, laptops, phones and digital devices. This includes flash drives, hard copies of client information and copiers.
- Identify all vendors you might use or share personal information with to complete a financial transaction, make a financial plan, or sell a product solution.
- Think about software that you use to complete financial plans, evaluate investments or store information – even temporarily – and any other times you work with sensitive data.
- Understand the entry and exit points for all your sensitive data. Do you use a local server or is your business tied to a larger server at your broker-dealer or corporate RIA? You must know and understand how your computers interact with all the sensitive data and who owns those sources.

> *"So, begin by taking inventory of all your "at risk" asssets.*

HOW TO PROTECT YOUR PRACTICE

Understanding what data you have will help you evaluate the risks associated with your business and your clients' personal information. You need a lot of your clients' information in order to make fiduciary recommendations; however, that doesn't mean you have to retain the risk of holding their personal data for extended periods of time. Know what information you need, when you need it, and for how long you need it. That can determine how you transfer the risk of personal data to another entity or retain the information for a holding period as required by regulatory agencies.

2. Scale Down

As a simple rule, "If you don't need it, get rid of it." You don't want to hold on to data that is no longer useful to you. Don't continue to take the same security measures because it was the way you were taught in the business or because your firm has been doing it that way for decades. Cyberthreats are ever-changing – you must stay ahead of the game.

To reduce potential threats, you must reduce or transfer the risk of housing sensitive data. Some important points to consider as you think about reducing the data you have onsite:

- Don't use Personal Identifiable Information (PII) as part of your client identification process. Look to assign an unrelated number to each client in your client relationship management software, data warehouse or financial planning software. If you are unsure if a data point is a PII, you may check Department of Labor guidelines and definitions at www.dol.gov/general/ppii.
- When you need information to complete a transaction, transfer it to the proper institution as quickly as possible while still meeting regulatory and governing body standards. Only retain it when required, and transfer it using encrypted methods.
- Develop an internal process to ensure your clients' most sensitive data is only accessed by the staff members who need it. Staff access to client data should be on an "as needed" basis.
- While you scale down on critical information, think about how you will transfer old data, destroy it once transferred, or retrieve it if it is needed again.
- If transferring data to cloud storage, make sure your providers have current SSL (Secure Sockets Layer) certificates.

> *If you don't need it, get rid of it.*

- When destructing data, make sure either your firm or the vendor you select completely destroys the data by shredding, pulverizing, or burning the information.
- Make sure data is encrypted every time you move it, especially when transferring it to a vendor.

The biggest step you can take in reducing your risk is to scale back on the data that you retain. The financial industry requires you to collect a lot of data to make informed decisions, but that doesn't mean you have to retain it unnecessarily. Understand what you have, then shift the risk to another party or completely get rid of the risk through proper destruction.

3. Lock It Down
Regulators and broker-dealers require financial professionals to retain certain data points for several years. You should check with your broker-dealer to see if you can shift some of the more sensitive information to their servers and away from your data center.

Understanding your key vulnerabilities is key to locking down information and making changes to your protocol. Just as you complete a repeatable process with each client for financial planning, you should install a repeatable process for handling your clients' sensitive and personal information.

Start by completing an audit of the potential risks in your protocol. It is strongly recommended that a full audit be completed by an outside authority; however, more frequent audits can be conducted by onsite personnel. What's key is that you identify what might happen and address those deficiencies before a cyber attacker beats you to the vulnerable parts of your security plans.

As you complete your audit, think about the hardware, software and people involved in data security.

Hardware
- Lock down electronic and paper information. Your paper file cabinets are just as vulnerable to threats as your computer. Any sensitive information – in any file – poses a risk to your clients' personal information.
- Keep all sensitive information in locked file cabinets. This includes paper files, thumb drives, and other discs with Personal Identifiable Information.

The biggest step you can take in reducing your risk is to scale back on the data that you retain.

HOW TO PROTECT YOUR PRACTICE

- Avoid keeping sensitive data on a computer that is connected to the Internet unless it is for normal business operations. Shift the data to more secure places once the business need is completed.
- Never leave your mobile device or laptop in a restaurant or in a car. If you must travel with a device, make sure it is secure and out of sight from any potential threat.
- As you upgrade your hardware, look for devices that require tokens, thumb prints, or other biometrics in addition to passwords.
- Your copier keeps a hard drive of the images that have been printed. Secure the printer just like you would a computer, especially during the disposal phase.

Software

- Identify all connections to your computers, laptops or mobile devices. Identify your servers and how they're protected – physically, through a back-up, and via a network firewall.
- Back up your data daily, if possible. If there are cost concerns, weekly might be better for your budget. But, you should be able to back up data for a reasonable expense.
- Always update your malware security programs. For more information about newly discovered vulnerabilities, check your vendor with www.us-cert.gov.
- Regularly review activity on your website. If you see a higher rate of visitors, you should investigate the source immediately. Also, look at requests for downloads. Many of your clients will request files of their holdings, but if the activity spikes, you should investigate the source of those requests and verify with your clients. Check for any activity that is not part of the normal course of business. (Think of this as you would re-balancing. You are looking for things out of alignment.)
- Consider multi-factor authentication for access to sensitive data about your clients. Having two steps of authentication makes it more difficult for a computer to dial into your systems and perpetrate a crime against your clients. Encourage your clients to use eight-character passwords with numbers and special characters as part of their access to their data.

Lock down electronic and paper info

Keep all sensitive information in locked file cabinets

Look for devices that require thumbprints or other biometrics

Secure the printer just like you would a computer

HOW TO PROTECT YOUR PRACTICE

People

- Your staff must adhere to "locking down" procedures with every client, every time, every day. Establish processes for who accesses the physical places where you store sensitive data. Consider keeping a log of highly sensitive data access by employee. If you rent space, make sure your commercial real estate manager understands your business and protects access to your office after hours.
- Disable employees' unauthorized programs and scan your office computers frequently for any unauthorized downloads.
- If you or your employees work remotely, look for Wi-Fi with protected access (WPA2) and use a VPN (Virtual Private Network). A new VPN system can be anywhere from free, up to a $75 annual subscription in most cases. More sophisticated packages are available for higher costs. Your broker-dealer should provide a VPN connection for you. This should be part of your due diligence questions when you search out new firms.

4. Pitch It

How many times have you walked by a trash bin and noticed copies of statements or other sensitive data that hasn't been completely destroyed? Too often, once you start noticing those things.

Criminals notice those things all the time. Be aware of how you dispose your sensitive data.

- Make sure your employees have access to proper places to dispose sensitive information that ultimately leads to the destruction of that material.
- Wipe information from computers when you upgrade hardware. This can include overwriting the entire hard drive so files are no longer retrievable.
- As the virtual trend grows, make sure your data destruction policies and procedures cover your remote employees. All employees should adhere to the same cybersecurity standards, regardless of location.

> *Be aware of how you dispose your sensitive data.*

HOW TO PROTECT YOUR PRACTICE

5. Plan Ahead

Establishing a plan for cybersecurity is just as important as establishing a business plan or your clients' financial plans. Knowing what to do in the event of a cyberthreat can greatly reduce stress for you and your clients. Your affected relationships will appreciate transparency and a quick reaction to any potential breach.

As you create your plan, here are some things to keep in mind:

- Your office should have a designated cybersecurity officer to investigate and coordinate your response plan.
- Consider whom you will have to notify of an event: clients, carriers, vendors, custodians, employees, and others. Secure those phone numbers in a separate location that is still locked down.
- If you suspect a cyberattack, disconnect your computers immediately. Assess the potential impacts to your office and clients immediately.
- Notify the appropriate people and address the issues head on. Make sure those affected know exactly what happened and what they need to do. Those things include checking their credit reports, checking account balances, and changing their passwords.

Suspect a Cyberattack?

1. **Disconnect your computers immediately**
2. **Assess the potential impacts to your office and clients**
3. **Contact your designated cybersecurity officer to investigate and coordinate your response plan**
4. **Secure phone numbers, contacts to those vendors, carriers and financial institutions in a different location**
5. **Notify the appropriate people and address the issues head on**

SUMMARY

By following the five steps outlined above, you will greatly reduce the risk of a cyberattack to your financial planning firm and your clients. It's important to remember that many of these key points don't require large investments of time, money or resources.

Much of this information comes from the FTC's "Protecting Personal Information: A Guide for Business."[5] Additionally, the FTC recommends the following resources for any small business concerned about securing sensitive data:

- Start with Security: www.ftc.gov/startwithsecurity
- OnGuard Online: www.ftc.gov/OnGuardOnline
- Small Business Administration: www.sba.gov/cyberseucrity
- Better Business Bureau: www.bbb.org/cybersecurity

It's important to remember that many of these key points don;t require large investments of time, money or resources.

[1] https://www.varonis.com/blog/cybersecurity-statistics/

[2] Barkly, "Security Confidence Headed Into 2017," December 2016: https://blog.barkly.com/cyber-attack-statistics-2016

[3] U.S. Department of Justice, Computer Crime and Intellectual Property Section, "How to Protect Your Networks from Ransomware: Interagency Technical Guidance Document," June 2016: https://www.justice.gov/criminal-ccips/file/872771/download

[4] Friedrich-Alexander University, "One in two users click on links from unknown senders," Aug. 25, 2016: https://www.fau.eu/2016/08/25/news/research/one-in-two-users-click-on-links-from-unknown-senders/

[5] Federal Trade Commission, "Protecting Personal Information: A Guide for Business," October 2016: https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-

About the Authors

MIKE MCGLOTHLIN, EVP, RETIREMENT - ASH BROKERAGE

Mike McGlothlin is a tireless advocate for the retirement planning industry. As executive vice president of retirement products at Ash Brokerage, he heads a team providing income planning solutions focused on longevity and efficiency. He also provides guidance and assistance for advisors and broker-dealers navigating marketplace and regulatory changes.

With more than 25 years of experience, Mike started his financial services career as a producer and qualified for the Million Dollar Round Table. Prior to joining marketing organizations as a distribution executive, he headed the national annuity distribution for a regional insurance marketing organization and a national brokerage general agency.

ANDREW DAHMAN, CHIEF TECHNOLOGY OFFICER - TECHFICIENT

As Chief Technology Officer at Techficient, Andrew leads the IT team with a mission to deliver the best, most efficient and secure experience for BGAs and their advisors. His passion is continually learning about the business in order to provide solutions through IT services and applications.

With more than 10 years of experience, his areas of expertise are application development and architecture. Key initiatives include creating a new core suite of enterprise systems, including an AMS (Agency Management System), CRM (Customer Relationship Management) system and customer portal while he was CIO at Ash Brokerage. Ash Brokerage took this industry leading software and spun it into a separate, independent organization called Techficient in 2020 and look to provide this same software to other BGAs.

DAVE BARCELONA, CHIEF INFORMATION SECURITY OFFICER - TECHFICIENT

As Chief Information Security Officer at Techficient, Dave leads our cybersecurity program and compliance. He creates and updates security policies, coordinates penetration tests, educates users on relevant topics, and maintains compliance with security standards.

Dave is a problem-solver. He enjoys learning about new technology as it develops, and he prides himself on keeping abreast of new IT security trends.

With more than 20 years of experience, he has experience in all areas of IT, ranging from development to infrastructure to security. Dave's experience and thorough knowledge across all areas helps him be more effective as a security leader and guiding the team to a robust security posture.

(800) 589-3000
ASHBROKERAGE.COM
10015 | Rev. 07/20

ASH BROKERAGE
Ash Answers.