The Truth About Cybersecurity

When it comes to securing critical data, what advisors don't know can hurt them.

The financial services industry is a honey pot: If someone wants to steal confidential information, they're not going to hack into a yogurt shop.

— Bridget Gaughan, chief information security officer for United Planners

Imagine arriving at your office one morning to find the front door wide open, broken glass on the floor. File cabinet drawers are pulled open, papers spilling out onto the ground. After the initial shock, your first concern likely is to determine what information was taken. Did the thieves make off with all of your clients' Social Security numbers? Are they already halfway across the country with a stack of brokerage account numbers tucked in their getaway bags?

This kind of scenario is a genuine fear for any advisor. After all, clients entrust their advisors with some of their most personal and confidential information — and it's the advisor's responsibility to keep that valuable information safe. That's why advisors use deadbolt locks, security systems and other physical protections to keep their offices safe. Yet many advisors fail to properly secure an even larger and potentially more vunerable target for thieves: their digital data.

The explosion of financial technology in recent years has benefited advisors in innumerable ways, but it also poses a big threat to advisors and their clients. Each year, thousands of incidents of cybercrime are reported in the financial services industry[1], and firms are devoting more resources to protecting critical data from increasingly sophisticated attacks. In fact, security spending rose nearly 70 percent from 2013 through 2016 as online threats have multiplied, regulatory expectations have increased and compliance policies have tightened in regard to how firms are expected to secure their digital data.

"This is an issue that advisors need to worry about," says Bridget Gaughan, chief information security officer for United Planners. "The financial services industry is a honey pot: If someone wants to steal confidential information, they're not going to hack into a yogurt shop. They know that financial service enterprises — including financial advisors — are a great place to go to get that information."

A Changing Environment

The ground rules have changed for financial advisors. As recently as a few years ago, advisors could rely on their

1 — PwC: https://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/financial-services-industry.html

tried-and-true strategies for working with clients. From the discovery meeting to the paper-heavy documentation of each new client's onboarding process, advisors knew how to operate. These days, however, advisors must increasingly navigate an industry landscape that's being reshaped by new regulations, demographic shifts and a surge in competition from alternative wealth management strategies.

Technology has been the answer to these challenges for many advisors. The right software can help advisors efficiently manage compliance issues and streamline operations. Online tools and digital communications can give clients a more user-friendly experience and make connections with back-office vendors more seamless. However, this increasing reliance on technology brings increased risks: Hackers may try to gain access to a firm's data by brute force, essentially breaking into the network through the exploitation of infrastructure weaknesses. They may also try to access client data through socially engineered phishing attacks — attempts to trick the firm's employees into giving up passwords and other critical data, often through fraudulent emails. "We're definitely seeing more incidents of hacking or data theft," says Gaughan. While advisors take these threats seriously, they often don't understand the complexity of the problem, or what resources are required to address it."

Gaughan says many advisors try to address their cybersecurity issues on the cheap. They may task the same IT vendor which fixes their office computers with developing a security system to withstand outside attacks. The problem is that those IT vendors may be underqualified and know very little about cybersecurity issues. Advisors may fail to ensure that their systems are constantly being updated through security patches and properly monitored. "They have the idea that they can check it once a year and be fine," says Gaughan, "but that inattention can leave them vulnerable."

The focus on the initial cost of software is a big issue for the advisory industry to address, says Aaron Spradlin, chief information officer at United Planners. That's because evaluating software or other technology primarily on price misses a key part of the equation: the strength of the security that's built into the software or the vendor's network. "The first question advisors should ask is how well the software secures their data," says Spradlin. "Unfortunately, that's usually the last question asked."

A Broken Model

Many advisors have taken an à la carte approach to building out their technology infrastructure, says Spradlin. Systems that include CRM platforms, client dashboards to back-office or compliance-related technologies are cobbled together using software from a number of vendors. While these pieces are designed to integrate with one another, each one might use a different data protection strategy.

Advisors with these types of patchwork technology systems are at a disadvantage. While some software

While advisors take these threats seriously, they often don't understand the complexity of the problem, or what resources are required to address it. They have the idea that they can check it once a year and be fine, but that inattention can leave them vulnerable.

— Bridget Gaughan, chief information security officer for United Planners

Ultimately a system is only as secure as its weakest link. You can't cobble together a system anymore. That model is dead... Regulators are handing out significant fines to firms that aren't following the rules for securing client data.

— Aaron Spradlin, chief information officer at United Planners

may have strong data protection, and some vendors may prioritize security, others may have looser standards. Ultimately, says Spradlin, a system is only as secure as its weakest link. A case in point: Lincoln Financial Group subsidiary was fined $650,000 by FINRA after lax security enabled hackers to access thousands of client records through a third-party vendor's cloud server. According to FINRA, Lincoln Financial didn't properly monitor that vendor's security capabilities. "In that case, it wasn't Lincoln Financial that was breached, but the third-party vendor," he says.

One reason there is such variance in security strength among different developers is the lack of any industry standard for security measures. While companies and industry groups are working to develop such a standard, Spradlin cautions that advisors should avoid piecing together such an à la carte system. "You can't cobble together a system like this anymore," he says. "That model is dead."

Instead, until a standard security protocol is developed, Spradlin suggests that advisors looking to upgrade their technology infrastructure consider providers that offer one-stop technology shopping. These offerings typically are from larger firms that have assembled turnkey solutions for advisors covering a wide variety of technology components, from CRM platforms to back-office administrative software. The benefit of this strategy, he says, is that the security of the system will be more uniform and, most likely, considerably safer than a system built with several unrelated software components.

This strategy may keep advisors from running afoul of regulatory issues. "These days, regulators are handing out significant fines to firms that aren't following the rules for securing client data," says Spradlin. Those rules include requiring firms to adopt written policies and procedures to protect client data from hackers and network breaches, as well as storage standards for data files.

Taking Action

Short of replacing their entire technology systems, what can advisory firms do to reduce the risk of cyberattacks? Step one is to make sure the firm has the personnel dedicated to managing security issues. That may mean hiring a chief information security officer (CISO) or working with a managed service provider that can create and execute a cybersecurity plan to protect the firm's technology infrastructure. That plan may include the use of VPNs — virtual private networks — which enable data to be securely sent and received through public or shared networks without being exposed. Endpoint protection is also a critical part of such a plan. Endpoint security software helps protect the network when it's accessed remotely through laptops, smartphones and other mobile devices.

Advisors also need to evaluate potential software vendors to deter-

Important Notes:

- Many vendors are limited liability companies that may not cover the cost of regulatory fines or other financial damages an advisory firm incurs in a cyberattack.
- Advisors should carry cybersecurity insurance to protect against fines and litigation stemming from the loss of client data if their current firm is not providing this for them.
- Training staff on cybersecurity is required.
- Have a written detailed plan on how you protect data and protocols to follow if a breach occurs.
- Appropriate due diligence of a vendor includes significant research pertaining to cyber security.

mine whether they meet the firm's bar for security. Spradlin says providers should at a minimum have completed a SOC 2 audit, which measures such things as the software's protection against unauthorized access. ("SOC" stands for Service Organization Controls, a reporting standard created by the American Institute of CPAs.)

Advisors also should create a checklist of questions to ask any potential technology vendors, including the following:

- How does the vendor or software protect data at rest?
- How is data in motion protected?
- Are there procedures in place to protect the software's code?
- Does the vendor have insurance to protect clients from financial damages, such as regulatory fines or civil litigation, in the event of a cyberattack?

The complete list of questions an advisory firm needs to ask potential vendors will vary from firm to firm. There's no standard bar that vendors need to clear to guarantee their products will be secure. For instance, Spradlin notes that many vendors are limited liability companies that may not cover the cost of regulatory fines or other financial damages an advisory firm incurs in a cyberattack. In recent years, firms such as RBC Capital Markets, SunTrust and Morgan Stanley have all faced fines of at least $1 million by the SEC or FINRA stemming from cybersecurity incidents. Wells Fargo Securities and Wells Fargo Prime Services in late 2016 were slapped with a combined $4 million in FINRA fines for failing to properly manage brokerage data.

As a result, advisors need to work with their CISO or managed service provider to create a list of criteria relevant to their firm — and to be able to evaluate the responses they get. "In recent years, we've seen a proliferation of vendors," says Gaughan. "Unfortunately, many of them haven't established the level of security that they need to have, so it's up to the advisor to know what questions to ask, and to know whether they receive the right answers."

Once a provider is selected, advisors should clarify the roles and responsibilities of that provider in a contract, says Spradlin. The contract should clearly state who is responsible or accountable for data security, and where the vendor's responsibility ends.

Finally, advisors should carry cybersecurity insurance to protect against fines and litigation stemming from the loss of client data if their current firm is not providing this for them. Spradlin says advisory firms will need to build — and follow — a cybersecurity plan to keep such a policy in effect.

Battling Behavior

Software vulnerabilities aren't the only ways hackers and other bad actors can abscond with critical client data. Gaining access to a firm's data repository

Human error is one of the biggest issues firms face. Many of these cybersecurity problems are caused by people making mistakes that expose the firm's information, such as clicking on an attachment that appears legitimate.
Email is a common point of entry for hackers," says Gaughan. "We will often send out fake emails to test advisors and educate them on the types of emails they shouldn't click on.

— Bridget Gaughan, chief information security officer for United Planners

can be as easy as sending a fake email to dupe a staffer into giving up passwords or other log-in credentials. Similarly, employees may forget to update operating systems or use easy-to-break passwords, essentially leaving the firm's virtual front door open to would-be thieves. "Human error is one of the biggest issues firms face," says Gaughan. "Many of these cybersecurity problems are caused by people making mistakes that expose the firm's information, such as clicking on an attachment that appears legitimate."

To that end, Gaughan urges companies to devote resources to educating staff about cybersecurity issues and the role they can play in keeping critical client data safe. That includes using secure devices and secure networks; making sure software such as virus protection and malware protection is up to date; using strong passwords; and making sure employees know how to spot fraudulent emails such as phishing attempts. "Email is a common point of entry for hackers," says Gaughan. "We will often send out fake emails to test advisors and educate them on the types of emails they shouldn't click on."

Gaughan also says advisors need to use common sense, and trust but verify when clients make out-of-the-ordinary requests. She remembers an advisor receiving a frantic email from a client requesting an immediate transfer of funds. The tone of the email wasn't typical of the client, and the advisor picked up the phone to call the client — and kept calling until the client answered. "It was over a long holiday weekend and the client was finally reached and said the request was legitimate," says Gaughan. "The advisor wasn't trying to make it hard for the client to get that money --- it was all about protecting the client."

To that end, Gaughan recommends advisors work closely with clients to discuss the measures the firm takes to protect their data — including requiring clients to speak with the advisor to confirm requests. Firms also should have a plan in place to alert clients and other parties if a cyberattack occurs. That incident response plan should include who to turn to for help — whether it is the firm that you are affiliated with (BD or RIA) or a software provider — as well as how to communicate issues to clients, regulators and others. "Advisors need to be able to tell clients whom to contact if they have concerns," says Gaughan. "It's always best to be proactive and reach out to clients, even for small incidents such as an email with sensitive information being sent to the wrong client."

Next StepsPlanning

There's no one-size-fits-all cybersecurity solution for financial advisors. Each firm has different needs and faces different threats. However, there is common ground: All advisors need to take a proactive approach to protecting their client's data, and build plans for their firms that recognize the constantly shifting nature of the technology environment. If they don't, advisors face a range of threats, from steep regulatory penalties to the catastrophic reputational

risks that can accompany these types of issues.

Fortunately, advisors don't need to do this work alone. For instance, United Planners offers advisors information on these issues in a dedicated Cybersecurity Resource Center on its advisor website platform called connectUP. United Planners also offers one-on-one guidance to help advisors build cybersecurity plans that fit their needs and address the unique security challenges that they face. "The good news is that there are a lot of people out there working on solving the cybersecurity problem," says Spradlin. "In the meantime, advisors need to take smart steps to give their clients and their firms the best protection they can. After all, this is no longer a threat that advisors can afford to ignore."

Independent, but Not Alone

United Planners understands advisors are independent contractors of the firm, and may choose from vast options for their technological needs. The firm's focus has been to assist advisors in maintaining their independent choices, while providing guidelines and safety through setting standards and protocols to keep the investing public's information safe. Sheila Cuffari-Agasi, senior vice president of United Planners Partner Development says, "Some firms are taking the approach to shut down options for advisors, causing them to rethink how they conduct business, while others are simply pretending this major threat doesn't exist. Most advisors are not technological engineers, and don't know where to begin to protect themselves. United Planners sees our role to assist advisors with their obligations of data security, while empowering systems and technology solutions that create efficiencies in conducting business safely."

Due diligence and the related costs of cybersecurity research and implementation can be overwhelming. United Planners has taken much of the burden off of associated advisors by providing turnkey solutions. Whether you go it alone or partner with a firm offering top-of-the-line solutions like United Planners, we urge you to face this issue — because what you don't know can hurt you.

The Future

Cybersecurity is not a "one and done" checklist. It requires constant evolution and improvement. Stay attuned with United Planners series of white papers and announcements for ***a very exciting launch of a new and innovative solution to protect confidential customer information brought to you through a co-op of financial services professionals*** (including firms, vendors, custodians and product providers) working in conjunction to deliver a secure, reliable and fast solution at an affordable price!

Following is a research tool United Planners has developed for our constituents that you may want to use to compare with your cybersecurity implementation costs:

Some firms are taking the approach to shut down options for advisors, causing them to rethink how they conduct business, while others are simply pretending this major threat doesn't exist... United Planners sees our role to assist advisors with their obligations of data security, while empowering systems and technology solutions that create efficiencies in conducting business safely.

— Sheila Cuffari-Agasi, senior vice president of United Planners Partner Development

Contact Partner Development for a consultation on how a unified approach to standardized security can be of value to you and your clients.

800-966-8737

UNITED PLANNERS FINANCIAL SERVICES

COMPARE YOUR CYBERSECURITY IMPLEMENTATION COSTS

CYBERSECURITY COST COMPARISON

OFFERING	AVG ANNUAL COST PER ADVISOR/OFFICE	COST THRU UNITED PLANNERS
Firewall, Encryption, Anti-Virus (malware/spyware) Weekly Reporting	$10,000 activation; $20-$55/device/month	First device covered in monthly $24.00 cost; $13/month for each additional device
Password Manager	$48/device/year	Included
Chief Information Security Officer *	$15,000 - $20,000 per year	Included
Cyber Insurance	$800 annual premium; $15,000 deductible; $250,000 limit	Included $5M policy; $5,000 RR deductible
Support Cost	$6,000 - $30,000	Included
Cybersecurity Education	$25-$100/year	Included
Certification of Compliance	Annual Audits - $500-$2,000	Included

ADMIN FEE COST COMPARISON

OFFERING	AVG ANNUAL COST PER ADVISOR/OFFICE	COST THRU UNITED PLANNERS
Due Diligence of Third Party Vendors/Technology	$5,000 per vendor	Use of vendors supported by United Planners included
Help Desk Support	$6,000 per year	Included
DOL Fiduciary Compliance*	$4,000 to $50,000	Included
ConnectUP / Single Sign On	$15,000	Included
Firm Element CE	$250	Included
Online Document Storage	$99-$299/M	Included
Email Monitoring, Storage & Hosting	$199 - $2,000/year	Included

COMPARE YOUR CYBERSECURITY IMPLEMENTATION COSTS

ADMIN FEE COST COMPARISON (continued)

OFFERING	AVG ANNUAL COST PER ADVISOR/OFFICE	COST THRU UNITED PLANNERS
Welcome, Annual Update and Change Confirmation Letters to Clients	$500 - $1,000 (est. $1 per letter for preparation, processing and postage expenses)	Included
Morningstar Annuity Intelligence Report	$600/year	Included
Straight Through Account Processing	$8,000-$15,000 set up fee	Included
Electronic Compensation Statements/Accounting & ACH payments 3x/month	$500/month	Included
AI Insight	$50/month	Included

*NOTE: All offerings include Independent RIAs except for those noted **

Contact Partner Development for a consultation on how a unified approach to standardized security can be of value to you and your clients.

800-966-8737

United Planners Financial Services
7333 E. Doubletree Ranch Road, Suite 120
Scottsdale, AZ 85258

UnitedPlanners.com